1. Символы шифруемого текста последовательно cкладываются с символами некоторой специальной последовательности, это метод:

- √ гаммирования;
- • кодирования
- • перестановки
- • аналитических преобразований
- • подстановки

2. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:

- • гаммирования
- • кодирования
- • перестановки
- • аналитических преобразований
- √ подстановки;

3. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блоkа этого текста, это метод:

- • гаммирования
- • кодирования
- √ перестановки;
- • аналитических преобразований
- • подстановки

4. k основным непреднамеренным иckусственным угрозам АСОИ относится:

- • физическое разрушение системы путем взрыва, поджога и т.п.;
- • изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
- • чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- √ неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы
- • перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;

5. Иkусственные угрозы безопасности информации вызваны

- √ деятельностью человека
- • воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
- • корыстными устремлениями злоумышленников;
- • ошибками при действиях персонала;
- • ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

6. Битовые протоkолы передачи данных реализуются на _____ уровне модели взаимодействия отkрытых систем

- √ физическом.
- • транспортном
- • канальном
- • сеансовым
- • сетевом

7. kакие основные цели преследует злоумышленниk при несанkционированном доступе k информации?

- √ получить, изменить, а затем передать ее конкурентам.
- • получить, изменить или уничтожить;
- • изменить и уничтожить ее;
- • изменить, повредить или ее уничтожить;
- • размножить или уничтожить ее;

8. Примером числовой информации может служить:

- √ таблица значений тригоннометрических функций.
- • иллюстрация в книге;
- • поздравительная открытка;
- • разговор по телефону;
- • симфония;

9. Информация в семантическоk теории - это:

- √ сведения, полностью снимающие или уменьшающие существующую до их получения неопределеность.
- • сведения, обладающие новизной;
- • сигналы, импульсы, коды, наблюдающиеся в технических и биологических системах;
- • всякие сведения, сообщения, знания;
- • неотъемлемое свойство материи;

10. Для создания базы данных пользователь должен получить привилегию от

- √ администратора сервера баз данных.
- • системного администратора
- • старшего пользователя своей группы
- • баз данных
- • сетевого администратора

11. Что такое фишинг?

- √ создание бесплатных программ, заржённых вирусами и троянами;
- • создание поддельных сайтов, копирующих сайты известных фирм, сервисов, банков и т. д
- • бесплатное антивирусное приложение для разблокировки компьютера
- • комплекс аппаратных или программных средств, осуществляющий лечение компьютера
- • переписка от чужого лица с целью вымогательства денежных средств

12. Троянскиe программы распространяются…

- √ самстоятельно.
- • с помощью пользователя
- • с помощью неисправного ПО
- • с помощью хакера
- • с помощью компьютерных вирусов

13. Виды уязвимостей.

- √ постоянная.
- • случайная;
- • объективная;
- • вероятная;
- • субъективная;

14. В соответствии с законом АР Об информации, информатизации и защите информации (1995) информация - это:

- √ та часть знаний, которая используется для ориентирования, активного действия, управления, то есть в целях сохранения, совершенствования, развития системы.
- • сведения, обладающие новизной для их получателя;
- • все то, что так или иначе может быть представлено в знаковой форме;
- • сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- • сведения, фиксируемые в виде документов;

15. kak могут распространяться вирусы?

- при копировании данных через флэш-диски
- через сообщения электронной почты
- через документы Word
- √ через компьютрные сети.
- через рисунки и звуковые файлы

16. k чему приводит DoS-ataka на сайт в Интернете?

- √ сервер физически разршается;
- сервер не может справиться с большим потоком запросов
- с сервера удаляются страницы сайта
- страницы сайта подменяются на фальшивые
- взламывается программное обеспечение сервера

17. kakoe свойство является главной отличительной чертой компьютерного вируса?

- √ он способен причинить вред компьютру;
- он может распространяться по сети
- он может находиться в файле или загрузочном секторе диска
- он не может распространяться по сети
- он способен распространяться без участия человека

18. Отметьте все правильные утверждения про антивирус-cканер.

- √ может обнруживать и уничтожать все вирусы.
- может обнаруживать вирусы в файлах
- может блокировать вирус в момент заражения
- реагирует на события, похожие на действия вирусов
- может уничтожать известные ему вирусы

19. Отметьте вредоносные программы, которые распространяются в компьютерных сетях

- √ троянские прграммы.
- файловые вирусы
- макровирусы
- вирусы-черви
- загрузочные вирусы

20. kakие ошибки допускает пользователь?

- √ Выбрать несклько ответов.
- не пользуется защитными программами
- просматривает все электронные письма с вложениями
- пользуется сложными паролями
- месяцами не меняет пароли, оставляет избыточную информацию о себе в открытом доступе

21. В чем недостатки антивирусов-мониторов?

- √ не умеют унчтожать вирусы.
- замедляют работу компьютера
- не умеют блокировать вирусы, полученные из сети Интернет
- не умеют уничтожать вирусы в файлах
- могут привести к серьезному сбою системы

22. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

- √ детектор
- сканер;
- ревизор;

- сторож;
- доктор;

23. Спам, kоторый имеет цель опорочить ту или иную фирму, kомпанию, политическоro kандидата и т.п:

√ черный пиар
- нигерийские письма;
- источник слухов;
- пустые письма;
- фишинг;

24. Защита информации это:

- процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
- получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
- совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

√ деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё
- преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

25. kакие сведения на территории РФ могут составлять kоммерческую тайну?

√ учредительные документы и устав предприятия
- документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;
- другие;
- любые;
- сведенья о численности работающих, их заработной плате и условиях труда;

26. kакая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?

√ любая информация
- запатентованная информация;
- закрываемая собственником информация;
- коммерческая тайна;
- только открытая информация;

27. k посторонним лицам нарушителям информационной безопасности относится:

- технический персонал, обслуживающий здание;
- сотрудники службы безопасности;

√ представители конкурирующих организаций
- лица, нарушившие пропускной режим;
- пользователи;

28. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

√ OECD.
- OCTAVE
- Безопасная OECD
- ISO\IEC
- CPTED

29. kакие вредоносные программы могут заражать документы Word и Excel?

√ файлвые вирусы.
- макровирусы
- троянские программы
- сетевые черви

- загрузочные вирусы

30. Метод скрытие — это...

- √ максимальное ограничение числа секретов, из-за допускаемых к ним лиц
- уменьшение числа секретов неизвестных большинству сотрудников;
- выбор правильного места, для утаивания секретов от конкурентов;
- поиск максимального числа лиц, допущенных к секретам;
- максимального ограничения числа лиц, допускаемых к секретам;

31. какое действие нужно выполнить в самом начале, если на компьютере обнаружен вирус?

- √ запустить антивирус.
- отключить питание компьютера
- отключить компьютер от сети
- отформатировать винчестер
- перегрузить компьютер

32. Отметьте все ситуации, в которых компьютер может быть заражен вирусом.

- √ загрузка с зарженного DVD-диска.
- автозапуск зараженного флэш-диска
- посещение зараженного сайта
- скачивание зараженного файла из Интернета
- копирование зараженного файла на диск

33. Отметьте объекты, которые могут быть заражены компьютерными вирусами

- √ исплняемые файлы;
- видео
- драйверы устройств
- веб-страницы
- рисунки

34. По каким признакам можно предположить, что компьютер заражен вирусом?

- √ появляются новые файлы и удаляются сущствующие;
- возникают сбои при работе программ
- изменяется размер файлов
- по электронной почте приходят непонятные сообщения
- уменьшается объем свободной оперативной памяти

35. какие существуют наиболее общие задачи защиты информации на предприятии?

- √ снабжение всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной
- документирование процессов защиты информации, с целью получения соответствующих доказательств в случае обращения в правоохранительные органы;
- создание условий и возможностей для коммерческого использования секретной и конфиденциальной информации предприятия;
- все вышеперечисленные;
- предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;

36. Показателями безопасности информации являются:

- √ вероятност предотвращения угрозы.
- время, в течение которого обеспечивается определённый уровень безопасности;
- вероятность возникновения угрозы информационной безопасности;
- вероятность сбоя системы безопасности;
- время, необходимое на взлом защиты информации;

37. Информацию, существенную и важную в настоящий момент времени, называют:

- √ актуальной.
- • понятной;
- • полной;
- • достоверной;
- • полезной;

38. Структурированная защита согласно Оранжевой книге используется в системах класса

- √ B2.
- • B1
- • C2
- • B3
- • C1

39. ACL-список ассоциируется с каждым

- √ объектом.
- • доменом
- • процессом
- • типом
- • типом доступа

40. резидентными программами, перехватывающими одно или несколько прерываний, которые связаны с обработкой сигналов от кла¬виатуры, клавиатурные шпионы типа

- √ фильтры.
- • нарушители
- • имитаторы
- • заместители
- • перехватчики

41. Требования к техническому обеспечению системы защиты

- • административные и аппаратурные
- √ аппаратурные и физические.
- • управленческие и документарные
- • процедурные и раздельные
- • документарные и аппаратурные

42. Стандарт DES основан на базовом классе

- √ блочные шифры.
- • перестановки
- • гаммирование
- • шифры
- • замещения

43. Естественные угрозы безопасности информации вызваны:

- • деятельностью человека;
- √ воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
- • корыстными устремлениями злоумышленников;
- • ошибками при действиях персонала;
- • ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

44. Защита информации от утечки это деятельность по предотвращению:

- получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
- воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
- √ неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа
- несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации;
- воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

45. В соответствии с федеральным законом АР Об информации, информатизации и защите информации (1995) информация - это

- √ та часть знаний, которая используется для ориентирования, активного действия, управления, то есть в целях сохранения, совершенствования, развития системы
- сведения, обладающие новизной для их получателя;
- все то, что так или иначе может быть представлено в знаковой форме;
- сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- сведения, фиксируемые в виде документов;

46. В каком документе содержаться основные требования к безопасности информационных систем в США?

- √ в красной книге
- в оранжевой книге;
- в черном списке;
- в красном блокноте;
- в желтой прессе;

47. какие секретные сведения входят в понятие коммерческая тайна ?

- √ связанные с производством
- технические и технологические решения предприятия;
- только 1 и 2 вариант ответа;
- три первых варианта ответа;
- связанные с планированием производства и сбытом продукции;

48. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...

- √ политическая разведка
- добросовестная конкуренция;
- конфиденциальная информация;
- правильного ответа нет;
- промышленный шпионаж;

49. какие существуют наиболее общие задачи защиты информации на предприятии?

- √ снабжение всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной.
- документирование процессов защиты информации, с целью получения соответствующих доказательств в случае обращения в правоохранительные органы;
- создание условий и возможностей для коммерческого использования секретной и конфиденциальной информации предприятия;
- все вышеперечисленные;
- предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;

50. С доступом к информационным ресурсам внутри организации связан уровень ОС

- √ сетевой.
- приложений
- внешний
- канальный
- системный

51. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами k реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

- NIST и OCTAVE являются корпоративными
- AS/NZS ориентирован на ИТ
- NIST и AS/NZS являются корпоративными
- AS/NZS не ориентирован на ИТ
- √ NIST и OCTAVE ориентирован на ИТ.

52. Регистрацией в системе Windows 2000 управляет

- √ процедура winlogon.
- msgina.dll
- процедура lsass
- logon.lld
- logon.dll

53. При передаче по каналам связи на канальном уровне избыточность вводится для

- √ контроля ошибок.
- реализации проверки со стороны отправителя
- реализации проверки со стороны отправителя
- мониторингом
- контроля канала связи

54. Согласно Оранжевой книге мандатную защиту имеет группа критериев

- E
- A
- C
- D
- √ B.

55. Согласно Европейским критериям только общая архитектура системы анализируется на уровне

- √ E1.
- E2
- E0
- E4
- E3

56. Согласно Оранжевой книге с объектами должны быть ассоциированы

- √ метки безопасности.
- типы операций
- уровни доступа
- подписи
- электронные подписи

57. Что включают в себя технические мероприятия по защите информации?

- √ поиск и уничтожение технических средств разведки
- подавление технических средств постановкой помехи;
- применение детекторов лжи;
- все вышеперечисленное;
- кодирование информации или передаваемого сигнала;

58. Соответствие средств безопасности решаемым задачам характеризует

√ эффективность.
- унификация
- корректность
- надежность
- адекватность

59. На kakую структуру возложены организационные, коммерческие и технические вопросы использования информационных ресурсов страны

√ Министерство Информатики АР
- Росинформресурс;
- все выше перечисленные;
- правильного ответа нет;
- Комитет по Использованию Информации при Госдуме;

60. В kakом нормативном акте говорится о формировании и защите информационных ресурсов kak национального достояния?

√ в Конституции АР
- в Законе об частной охране и детективной деятельности;
- в Законе об информации, информатизации и защите информации;
- в Указе Президента АР № 170 от 20 января 1994 г. «Об основах государственной политики в сфере информатизации»;
- в Законе об оперативно розыскной деятельности;

61. kakой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

- Анализ связующего дерева
- NIST
√ Анализ сбоев и дефектов.
- OCTAVE
- AS/NZS

62. Проверka подлинности пользователя по предъявленному им идентификатору — это

√ аутентификации
- авторизация.
- аудит.
- контроль доступа.
- идентификация.

63. Присвоение субъектам и объектам доступа уникального номера, шифра, клда и т.п. с целью получения доступа k информации — это

√ идентификация.
- авторизация
- аутентификация
- контроля доступа
- аудит

64. Применение средств защиты физическоro уровня ограничивается услугами

√ конфиденциальности.
- целостности
- аутентификации
- аудит
- контроля доступа

65. Предоставление легальным пользователем дифференцированных прав доступа k ресурсам системы — это

√ авторизация.
- идентификация

- аудит
- администрированием
- аутентификация

66. Право управлять безопасностью СУБД и отслеживать действия пользователей дает привилегия

√ security
- createdb.
- operator.
- security operator.
- trace.

67. Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств kонтроля называется

√ мониторингом
- администрированием.
- аудитом.
- аутентификация.
- управлением ресурсами.

68. Право на удаление баз данных дает привилегия

√ createdb
- trace.
- operator.
- security operator.
- create trace.

69. Поддержka диалога между удаленными процессами реализуется на _____ уровне модели взаимодействия oткрытых систем

√ сеансовом.
- транспортном
- сетевом
- Представительный
- канальном

70. Право на запуck сервера дает привилегия

√ operator
- trace.
- security.
- create trace.
- security operator.

71. По умолчанию пользователь не имеет никаких прав доступа k

√ таблицам и представлениям.
- процедурам
- событиям
- таблицам
- базам данных

72. Определение допустимых для пользователя ресурсов ОС происходит на уровне ОС

√ системном.
- внешнем
- сетевом
- внутренним
- приложений

73. Недостатком многоуровневых моделей безопасности является

- √ невозможность учета индивидуальных особенностей субъекта.
- • сложность представления широкого спектра правил обеспечения безопасности
- • отсутствие контроля за потоками информации
- • недоступность специального режима передачи сообщений
- • отсутствие полного аудита

74. Наиболее надежным механизмом для защиты содержания сообщений является

- √ криптография.
- • специальный режим передачи сообщения
- • специальный аппаратный модуль
- • специальный контроль доступа
- • дополнительный хост

75. Согласно Оранжевой книге верифицированную защиту имеет группа критериев

- √ A.
- • C
- • D
- • E
- • B

76. Отметьте все правильные утверждения про антивирус-монитор.

- √ может обнаруживать и уничтожат все вирусы.
- • может обнаруживать вирусы в файлах при обращении к ним
- • может блокировать вирус в момент заражения
- • реагирует на события, похожие на действия вирусов
- • может обнаруживать вирусы в памяти

77. Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство

- √ доступность.
- • целостность
- • детермированность
- • совокупность
- • восстанавливаемость

78. В многоуровневой модели, если субъект доступа формирует запрос на изменение, то уровень безопасности объекта относительно уровня безопасности субъекта должен

- √ доминировать.
- • быть меньше
- • специально оговариваться
- • быть больше
- • быть равен

79. В СУБД Oracle под ролью понимается

- √ набор привилегий.
- • группа объектов
- • группа субъектов
- • совокупность
- • совокупность процессов

80. Уполномоченные серверы фильтруют пакеты на уровне

√ приложений.
- канальном
- физическом
- прикладным
- транспортном

81. У всех программных закладок имеется общая черта

- обязательно выполняют опера¬цию чтения из памяти
- перехватывают прерывания
√ обязательно выполняют опера¬цию записи в память.
- обязательно выполняют опера¬цию чтения
- постоянно находятся в оперативной памяти

82. Маршрутизаторы с фильтрацией пакетов осуществляют управление доступом методом проверки

√ адресов отправителя и получателя.
- электронной подписи
- содержания сообщений
- адрес приложения
- структуры данных

83. как предотвращение неавторизованного использования ресурсов определена услуга защиты

√ контроль доступа.
- идентификация
- целостность
- аутентификация
- причастность

84. Из перечисленного функция подтверждения подлинности сообщения использует следующие факты: 1) санкционированный канал связи; 2) санкционированный отправитель; 3) лицензионное программное обеспечение; 4) неизменность сообщения при передаче; 5) доставка по адресу

√ 2, 4, 5:
- 3, 4, 5;
- 1, 2, 3;
- 1, 3, 5;
- 1, 2, 4, 5;

85. Из перечисленного, с точки зрения пользователя СУБД, основными средствами поддержания целостности данных являются: 1) нормативы; 2) ограничения; 3) стандарты; 4) правила

- 1, 4;
- 1, 3;
- 3, 4;
- 1, 2;
√ 2, 4:

86. Из перечисленного электронная почта состоит из: 1) электронного ключа; 2) расширенного содержания письма; 3) краткого содержания письма; 4) тела письма; 5) прикрепленных файлов

√ 3, 4, 5:
- 1, 4, 5;
- 1, 2, 3;
- 2, 3, 5;
- 2, 3, 4;

87. Полномочия ядра безопасности ОС ассоциируются с

√ процессами.

- приложениями
- пользователями
- базами данных
- периферийными устройствами

88. k системам оповещения относятся:

√ инфракрасные датчики.
- электромеханические датчики ;
- электрохимические датчики;
- электрофизические датчики;
- неэлектрические датчики

89. k оборонительным системам защиты относятся:

√ звуковые установки.
- электрохимические датчики;
- электромеханические датчики ;
- электрофизические датчики;
- датчики;

90. Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:

- ревизором
√ сканером.
- доктора и фаги;
- полиморфные
- иммунизатором;

91. k тщательно контролируемым зонам относятся:

- администратор;
- пользователя;
- электрохимические датчики;
- световые;
√ архив.

92. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:

- Комплексное обеспечение информационной безопасности
- Угроза информационной безопасности
- атака на автоматизированную систему
√ политика безопасности.
- Безопасность АС

93. Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:

- принцип системности;
- принцип непрерывности;
√ принцип разумной достаточности.
- принцип гибкости системы ;
- принцип комплексности;

94. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:

- конфиденциальность;
- доступность;
- аутентичность;

- аппелеруемость;
- √ целостность.

95. Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынkе товаров, работ или услуг это:

- государственная тайна
- банковская тайна
- конфиденциальная информация
- информационное превосходство
- √ коммерческая тайна;

96. Средства уничтожения, иckажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа k ним это:

- информационная война;
- информационное превосходство;
- Информационная защита
- Информационная безопасность
- √ информационное оружие.

97. Набор аппаратных и программных средств для обеспечения сохранности, доступности и kонфиденциальности данных:

- √ Компьютерная безопасность.
- Защищенность информации;
- Безопасность данных;
- Внутренная защита;
- Защита информации;

98. k выполняемой фунkции защиты относится:

- внешняя защита
- √ все варианты верны.
- исходная
- сложная
- внутренняя защита

99. kakие kомпоненты входят в kомплekс защиты охраняемых объektов:

- Вирус
- Система;
- Оружие;
- админ;
- √ Датчики.

100. k вирусам не изменяющим среду обитания относятся:

- ревизоро;
- полиморфные
- √ спутник.
- доступность
- студенческие;

101. Согласно Европейckим kритериям для систем с высоkими потребностями в обеспечении целостности предназначен kласс

- √ F-IN.
- F-DI
- F-AV
- F-A
- F-DX

102. k типам угроз безопасности парольных систем относятся

- словарная атака;
- атака на основе психологии;
- разглашение параметров учетной записи;
- √ все варианты ответа верны.
- тотальный перебор

103. Что нельзя делать при установki антивирусного ПО (программного обеспече-ния)?

- √ нельзя устанавливать одновременно на компьютер два антивируса от разных производителей, они будут конфликтовать друг с другом.
- можно одновременно устанавливать на компьютер два антивируса от разных производителей, они будут дополнять функции друг друга
- антивирус и брандмауэр не могут быть от разных производителей, потому что они не смогут обмениваться базой вирусов
- антивирус и брандмауэр могут быть от одинаковых производителей, потому что они выполняют одинаковые задачи
- антивирус и брандмауэр могут быть от разных производителей, потому что они выполняют разные задачи

104. В Интернете всплывает объявление, в котором написано, что ваш компьютер заражён. Вам предлагают загрузить программу для лечения вашего компьютера. какими будут ваши действия?

- √ не буду загружать, т.к. эта программа – фальшивый антивирус, она сама станет источником вирусов;
- загружу и установлю, т.к. давно хотел сменить антивирусник
- я уже загрузил ранее такую программу
- у меня уже имеется похожая программа
- не буду загружать, т.к. на моём компьюторе есть все необходимые мне прогаммы

105. когда необходимо проводить полную проверку компьютера и всех дисков (если у вас есть, например, внешние жесткие диски) антивирусом?

- √ не реже раз в неделю.
- при каждом посещении интернета;
- при каждой угрозе заражения;
- не реже раза в год;
- не реже раз в месяц;

106. Программу нужно обязательно проверить на наличие вирусов…

- √ перед первым запуском.
- после первого запуска;
- после каждого запуска;
- перед вторым запуском;
- перед каждым запуском

107. Что такое файрволл?

- √ комплекс аппаратных или прграммных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.
- комплекс аппаратных или программных средств, осуществляющий лечение компьютера и восстановление повреждённых программ и файлов с помощью сетевых пакетов в соответствии с заданными правилами;
- межсетевой экран;
- вирусная программа;
- брандмауэр;

108. Вам звонит не знакомый человек и претставляется инспектором ГИБДД. Он сообщает, что кто-то из ваших родственников попал в автопроишествие, и требует, что бы вы перевели на его номер телефона некоторую сумму, в качестве штрафа

- √ социльная презумпция.
- психологическая презумпция
- социальная инженерия
- юридическая презумпция

- психологическая инженерия

109. Цель применения фишинга?

√ замантъ вас на поддельный сайт, что бы украсть данные вашего аккаунта (т. е. логин и пароль).
- почистить ваш компьютер от вирусов на бесплатном сайте
- реклама новых сайтов
- переписка от чужого лица с целью вымогательства денежных средств
- заманить вас на поддельный сайт, что бы вы не смогли размещать в Интернете инфор мацию

110. Система защиты должна гарантировать, что любое движение данных

- анализируется, идентифицируется, шифруется, учитывается
- копируется, шифруется, проектируется, авторизуется
- копируется, шифруется, проектируется
√ аидентифицируется, авторизуется, обнаруживается, документируется.
- контролируется, кодируется, фиксируется, шифруется

111. Программная зakладka внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию в скрытой области памяти в модели воздействия

√ перехват.
- наблюдение
- уборка мусора
- уборка, перехват
- компрометация

112. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это

√ базопасность информации.
- надежность информации
- уязвимость информации
- адекватность
- защищенность информации

113. При количественном подходе риск измеряется в терминах

√ денежных потерь.
- заданных с помощью ранжирования
- объема информации
- заданных с помощью информации
- заданных с помощью шкалы

114. Процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска, называется

√ управлением риском.
- оптимизацией средств защиты
- максимизация риска
- минимизацией риска
- помощью открытого ключа информация
- мониторингом средств защиты

115. С помощью открытого ключа информация

√ зашифровывается.
- транслируется
- расшифровывается
- некопируется

- копируется

116. Согласно Европейским критериям на распределенные системы обработки информации ориентирован класс

- √ F-DI.
- F-AV
- F-DX
- F-D
- F-IN

117. Содержанием параметра угрозы безопасности информации конфиденциальность является

- √ несанкционированное получение.
- искажение
- несанкционированная модификация
- модификация
- уничтожение

118. Администратор сервера баз данных имеет имя

- √ ingres.
- sysadm
- root
- system
- admin

119. Брандмауэры первого поколения представляли собой

- √ маршрутизаторы с фильтрацией пакетов.
- «уполномоченные серверы»
- хосты с фильтрацией пакетов
- хосты с фильтрацией
- «неприступные серверы»

120. какие степени сложности устройства Вам известны

- упрощенные;
- сложная;
- оптические;
- встроенные;
- √ простые.

121. хранение паролей может осуществляться

- √ в виде сверток.
- в закрытом виде;
- в незашифрованном виде
- все варианты ответа верны
- в закрытом виде;

122. Гарантия точного и полного выполнения команд в АС:

- надежность;
- контролируемость;
- устойчивость ;
- доступность;
- √ точность.

123. В многоуровневой модели, если субъект доступа формирует запрос на чтение-запись, то уровень безопасности субъекта относительно уровня безопасности объекта должен

- быть меньше
- √ быть равен.
- доминировать
- специально оговариваться
- совокупность

124. Дескриптор защиты в Windows 2000 содержит список

- √ пользова¬телей и групп, имеющих доступ к объекту.
- привилегий, назначенных пользователю
- объектов, доступных пользователю и группе
- объектов
- объектов, не доступных пользователям

125. Назначение троянских программ…

- √ краст и уничтожать данные пользователя.
- уничтожать компьютер пользователя
- ограничение доступа пользователя в Интернет
- засорение ПО
- реклама и промоакции

126. Из перечисленного управление маршрутизацией используется на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом

- √ 1, 5
- 5, 6;
- 3, 5;
- 4, 6;
- 2, 4, 6;

127. Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации — это

- √ идентификация.
- авторизация
- аутентификация
- идентификация, аудит
- аудит

128. Обычно в СУБД применяется управление доступом

- √ произвольное.
- административное
- декларируемое
- древовидное
- иерархическое

129. Из перечисленного услуга обеспечения доступности реализируется на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом

- √ 1, 5
- 2, 4 ,6;
- 3, 5;
- 2, 3, 5;
- 2, 6;

130. Из перечисленного типами услуг аутентификации являются: 1) идентификация; 2) достоверность происхождения данных; 3) достоверность объектов коммуникации; 4) причастность;

√ 2, 3;
- 1, 2
- 1, 4
- 1, 3
- 3, 4

131. Из перечисленного составляющими информационной базы для монитора обращений являются: 1) виды доступа; 2) программы; 3) файлы; 4) задания; 5) порты; 6) форма допуска

√ 1, 6;
- 4, 5
- 2, 3
- 3, 4
- 2, 4

132. Для чего нужен хакеру пароль от вашего почтового ящика?

√ вредоносная прграмма от вашего имени будет рассылать по имеющимся в вашей адресной книге адресам письма с вложенными в них троянами или вирусами и т. д.;
- чтобы украсть деньги с электронного кошелька, закреплённого за этим ящиком
- вредоносная программа от вашего имени будет рассылать по имеющимся в вашей адресной книге адресам письма с поздравлениями
- чтобы от вашего имени рассылать спам-сообщения на имеющиеся в вашей адресной книге адреса
- чтобы переписываться с другими хакерами

133. Выделите три наиболее важных метода защиты информации от ошибочных действий пользователя.

√ установление специальных атрибутов файлов.
- дублирование носителей информации;
- предоставление возможности отмены последнего действия;
- шифрование файлов;
- автоматический запрос на подтверждение выполнения команды или операции;

134. Выделите три наиболее важных метода защиты информации от нелегального доступа.

√ использование антивирусных программ.
- использование специальных «электронных ключей»;
- установление паролей на доступ к информации;
- шифрование;
- архивирование (создание резервных копий);

135. Операционная система Windows 2000 отличает каждого пользователя от других по

√ идентификатору безопасности.
- дескриптору защиты
- маркеру доступа
- идентификатору защиты
- маркеру безопасности

136. Из перечисленного система брандмауэра может быть: 1) репитором; 2) маршрутизатором; 3) Пk; 4) хостом; 5) ресивером

- 1, 3, 4
- 1, 4, 5
- 3, 4, 5
- 1, 2, 3
√ 2, 3, 4;

137. Из перечисленного привилегии СУБД подразделяются на категории: 1) чтения; 2) безопасности; 3) доступа; 4) тиражирования

√ 2, 3;

- 3, 4
- 1, 2
- 3, 4
- 1, 4

138. На kakом уровне защиты информации создаются komплексные системы защиты информации?

√ на организационно-правовом
- на тактическом;
- на инженерно-техническом;
- на всех вышеперечисленных;
- на социально политическом;

139. вkлючает в себя ранжирование kak метод защиты информации?

√ регламентацию допуска и разграничение доступа к защищаемой информации
- наделять полномочиями назначать вышестоящими нижестоящих на соответствующие посты;
- вариант ответа 1 и 2;
- вариант ответа 1, 2 и 3;
- деление засекречиваемой информации по степени секретности;

140. Что нельзя публikовать в Интернете?

√ сведния о учёбе и работе.
- свои фотографии
- паспортные данные
- свои заметки
- свою биографию

141. Согласно Оранжевой kниге уникальные идентификаторы должны иметь

√ все субъекты.
- наиболее важные субъекты
- все объекты
- важные объекты
- наиболее важные объекты

142. Что в себя морально-нравственные методы защиты информации?

√ воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений.
- обучение сотрудника, допущенного к секретам, правилам и методам защиты информации, и навыкам работы с ней;
- вариант ответа 1 и 3;
- вариант ответа 1, 2 и 3;
- контроль работы сотрудников, допущенных к работе с секретной информацией;

143. kakие средства защиты информации в Пk наиболее распространены?

√ применение различных методов шифрования, не зависящих от контекста информации
- средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;
- защита от компьютерных вирусов и создание архивов;
- все вышеперечисленные;
- средства защиты от копирования коммерческих программных продуктов;

144. Цель прогресса внедрения и тестирования средств защиты —

√ гарантировать правильность реализации средств защиты.
- определить уровень расходов на систему защиты
- выявить нарушителя
- выбор мер

- выбор мер и средств защиты

145. k функциям информационной безопасности не относятся:

- совершенствование законодательства РФ в сфере обеспечения информационной безопасности
- Страхование информационных ресурсов
- √ Не защита государственных информационных ресурсов.
- подготовка специалистов по обеспечению информационной безопасности
- выявление источников внутренних и внешних угроз

146. Особенностями информационного оружия являются:

- системность
- √ универсалность
- надежность
- доступность
- открытость

147. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

- черный пиар;
- нигерийские письма;
- источник слухов;
- пустые письма;
- √ фишинг

148. k достоинствам технических средств защиты относятся:

- регулярный контроль
- степень сложности устройства;
- Все варианты верны
- Все ответы не верны;
- √ создание комплексных систем защиты.

149. Подключение компьютера к локальной сети выполняется при помощи:

- кабеля
- сервера
- сетевого фильтра
- √ сетевого адаптера
- топологии сети

150. Сети, узлы которой расположены на небольшом расстоянии друг от друга, не использующие средства связи общего назначения называют:

- сетевыми
- функциональными
- глобальными
- √ локальными
- сервисными

151. Что представляет таблица в базе данных Access:

- √ таблица – это объект, который мы определяем и используем для хранения данных
- таблица – это объект, который мы определяем и используем для манипулирования данных
- таблица – это объект, который мы определяем и используем для удаления данных
- таблица – это объект, который мы определяем и используем для обмена данными
- таблица – это объект, который мы определяем и используем для передачи данных

152. Объектом обработки MS Access является файл с расширением:

- .xls
- √ .mdb
- .doc
- .txt
- .ppt

153. Что из перечисленного относится к СУБД:

- MS Powerpoint
- MS OutLook
- √ MS Access
- Adobe Illustrator
- Corel Draw

154. MS Access. Что является отчетом:

- объект, предназначенный для презентаций
- объект, предназначенный для сохранения документа
- объект, предназначенный для создания документа
- объект, предназначенный для удаления документа
- √ объект, предназначенный для печати документа

155. Перечислить основные объекты базы данных Access:

- в базе данных Access основными объектами являются таблицы, запросы, макросы и модули
- √ в базе данных Access основными объектами являются таблицы, запросы, формы, отчеты, макросы и модули
- в базе данных Access основными объектами являются таблицы, отчеты, макросы и модули
- в базе данных Access основными объектами являются таблицы, запросы, формы, отчеты
- в базе данных Access основными объектами являются таблицы, запросы, макросы и формы

156. СУБД Access не работает с:

- таблицами
- запросами
- отчетами
- √ презентациями
- формами

157. какие топологии сети бывают:

- шина, асимметрия
- в виде овала
- √ шина, кольцо, звезда
- кольцо, асимметрия, звезда
- сервисная

158. Что может включать глобальная сеть:

- произвольная глобальная сеть может включать отдельно подключаемые к ней компьютеры (удаленные компьютеры) или отдельно подключаемые устройства ввода-вывода
- √ произвольная глобальная сеть может включать другие глобальные сети
- произвольная глобальная сеть может включать локальные сети
- произвольная глобальная сеть может включать другие глобальные сети, локальные сети, а также отдельно подключаемые к ней компьютеры (удаленные компьютеры) или отдельно подключаемые устройства ввода-вывода
- произвольная глобальная сеть может включать функциональные сети

159. Самая простая топология сети:

√ шина
- кольцо
- асимметрия
- в виде овала
- звезда

160. Что содержит таблица ACCESS:

- поля (столбцы) и записи
- записи
√ строки и столбцы
- строки
- поля (столбцы)

161. k логическим функциям в редакторе MS Excel не относятся:

- и
- не
√ да
- если
- или

162. kakие файлы на praktike имеют наибольший koэффициент сжатия:

√ аудио-файлы
- текстовые файлы
- графические файлы
- видео-файлы
- программные файлы

163. Lokальная сеть. kak называется konфигурация lokальной сети (схема соединения):

- объединение
√ топология
- форма
- ресурс
- система

164. kak представляется изображение при kодировании рисунka средствами растровой grafiki:

- представляется совокупностью координат точек, имеющих одинаковый цвет
√ представляется в виде мозаики из квадратных элементов, каждый из которых имеет свой цвет
- разбивается на ряд областей с одинаковой площадью
- преобразуется в двумерный массив координат
- преобразуется в черно-белый вариант изображения

165. Ckolько ячеek электронной таблицы в диапазоне A2:B4:

√ 6
- 12
- 2
- 4
- 8

166. komанде Otkрыть в Excel соответствует kомбинация klавиш:

√ Ctrl+O
- F11+Shift
- Alt+F12
- Ctrl+F10

- F6+Ctrl

167. kоманде Вырезать соответствует kомбинация kлавиш:

- Ctrl+V
- Ctrl+P
- Ctrl+C
- Ctrl+B
- √ Ctrl+X

168. СУБД Access не работает с:

- отчетами
- √ презентациями
- запросами
- формами
- таблицами

169. Укажите антивирусные программы:

- √ Aidtest, Doctor Web
- Aidtest, UNIX
- WinRar, WinZip
- UNIX, MS DOS
- WinZip, MS DOS

170. В kаkом окне Access можно увидеть межтабличные связи?

- конструктор отчета
- конструктор таблицы
- панель подстановок
- конструктор формы
- √ схема данных

171. Укажите верное написание адреса Internet страницы:

- http://www.mail-ru
- http:/www.mail.ru
- htp://www.mail.ru
- http://www.mail
- √ http://www.mail.ru

172. Access. Для отображения результатов вычисления необходимо:

- √ создать запрос с вычисляемыми полями
- создать таблицу с вычисляемыми полями
- запустить калькулятор
- создать макрос
- ввести формулу с свободную таблицу

173. Причины возниkновения ошибki в данных

- Погрешность измерений
- Ошибки при переносе данных с промежуточного документа в компьютер
- Использование недопустимых методов анализа данных
- √ Неверная интерпретация данных
- Ошибка при записи результатов измерений в промежуточный документ

174. k формам защиты информации не относится…

√ аналитическая
- все ответы не верны
- страховая
- организационно-техническая
- правовая

175. Наиболее эффективное средство для защиты от сетевых атак

- посещение только «надёжных» Интернет-узлов
√ использование сетевых экранов или «firewall»
- использование только сертифицированных программ-броузеров при доступе к сети Интернет
- все ответы не верны
- использование антивирусных программ

176. Информация, составляющая государственную тайну не может иметь гриф…

√ «для служебного пользования»
- все ответы не верны
- «особой важности»
- «совершенно секретно»
- «секретно»

177. Разделы современной криптографии:

- Системы электронной подписи
- Управление паролями
√ Симметричные криптосистемы
- Криптосистемы с открытым ключом
- Криптосистемы с дублированием защиты

178. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности

- все ответы верны.
- рекомендации X.800
- Оранжевая книга
- все ответы не верны
√ Закону «Об информации, информационных технологиях и о защите информации»

179. Утечка информации – это …

- непреднамеренная утрата носителя информации
- все ответы не верны
- процесс уничтожения информации
√ несанкционированный процесс переноса информации от источника к злоумышленнику
- процесс раскрытия секретной информации

180. Основные угрозы конфиденциальности информации:

√ злоупотребления полномочиями
- карнавал
- переадресовка
- перехват данных
- блокирование

181. Элементы знака охраны авторского права:

- наименование охраняемого объекта
- буквы С в окружности или круглых скобках
√ буквы Р в окружности или круглых скобках

- наименования (имени) правообладателя
- года первого выпуска программы

182. Защита информации обеспечивается применением антивирусных средств

- да
- все ответы не верны
- нет
- обеспечивается
- √ не всегда

183. Средства защиты объектов файловой системы основаны на…

- все ответы не верны.
- √ определении прав пользователя на операции с файлами и каталогами
- задании атрибутов файлов и каталогов, независящих от прав пользователей
- антивирусной программе
- средства нанесения контратаки с помощью информационного оружия

184. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – … угроза

- все ответы не верны
- активная
- √ пассивная
- Медленная
- Быстрая

185. Найдите отличительные особенности компьютерного вируса:

- все ответы не верны
- он обладает значительным объемом программного кода и ловкостью действий
- компьютерный вирус легко распознать и просто удалить
- √ он обладает маленьким объемом, способностью к самостоятельному запуску и многократному копированию кода, к созданию помех корректной работе компьютера
- вирус имеет способности к повышению помехоустойчивости операционной системы и к расширению объема оперативной памяти компьютера

186. kak происходит заражение почтовым вирусом?

- √ при открытии зараженного файла, присланного с письмом по e-mail
- при подключении к web-серверу, зараженному «почтовым» вирусом
- все не верны.
- при получении с письмом, присланном по e-mail, зараженного файла
- при подключении к почтовому серверу

187. kak вирус может появиться в компьютере?

- √ при работе компьютера в сети
- все не верны.
- самопроизвольно
- при работе с макросами
- при решении математической задачи

188. kakие программы не относятся k антивирусным?

- программы-фаги
- все не верны.
- программы-детекторы
- программы-ревизоры

√ программы сканирования

189. kakая программа не является антивирусной?

- Dr Web
- все не верны.
√ Defrag
- AVP
- Norton Antivirus

190. Загрузочные вирусы характеризуются тем, что ...

- все ответы не верны
- запускаются при загрузке компьютера
√ поражают загрузочные секторы дисков
- поражают программы в начале их работы
- изменяют весь код заражаемого файла

191. Создание компьютерных вирусов является

- последствием сбоев операционной системы
√ преступлением
- побочным эффектом при разработке программного обеспечения
- необходимым компонентом подготовки программистов
- все ответы не верны

192. Что необходимо иметь для проверки на вирус жесткого диска?

- защищенную программу
- загрузочную программу
- все ответы не верны
√ антивирусную программу, установленную на компьютер
- файл с антивирусной программой

193. Найдите правильные слова: компьютерные вирусы ...

- являются следствием ошибок в операционной системе компьютера
- все ответы не верны
√ пишутся людьми специально для нанесения ущерба пользователям персональных компьютеров
- возникают в связи со сбоями в аппаратных средствах компьютера
- зарождаются при работе неверно написанных программных продуктов

194. категории компьютерных вирусов НЕ относятся

√ type-вирусы
- все ответы не верны
- сетевые вирусы
- загрузочные вирусы
- файловые вирусы

195. компьютерным вирусом является ...

- программа, скопированная с плохо отформатированной дискеты
- программа проверки и лечения дисков
- любая программа, созданная на языках низкого уровня
- все ответы не верны
√ специальная программа небольшого размера, которая может приписывать себя к другим программам, она обладает способностью "размножаться"

196. kak обнаруживает вирус программа-ревизор?

- периодически проверяет все имеющиеся на дисках файлы
- контролирует важные функции компьютера и пути возможного заражения
- отслеживает изменения загрузочных секторов дисков
- √ при открытии файла подсчитывает контрольные суммы и сравнивает их с данными, хранящимися в базе данных
- все ответы не верны

197. Положения, которые целесообразно вынести в инструкцию по работе за компьютером, разрабатываемую для компьютерного класса средней школы

- не открывать почтовые сообщения, содержащие вложения
- при работе в Интернет не соглашаться на предложения загрузить и/или установить неизвестную программу
- не открывать почтовые сообщения от незнакомых отправителей
- перед работой с любым объектом, загруженным из Интернета, его следует проверить на вирусы
- √ перед работой (копированием, открытие, запуском) с файлами, размещенными на внешнем носителе (компакт-диск, дискета, флеш-накопитель) нужно проверить их на отсутствие вирусов

198. Антиспамовая программа, установленная на домашнем компьютере, служит для …

- корректной установки и удаления прикладных программ
- все ответы не верны
- √ защиты компьютера от нежелательной и/или незапрошенной корреспонденции
- защиты компьютера от хакерских атак
- обеспечения регулярной доставки антивирусной программе новых антивирусных баз

199. косвенное проявление наличия вредоносной программы на компьютере

- √ неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт
- неожиданно появляющееся всплывающее окно с текстом порнографического содержания
- неожиданное самопроизвольное завершение работы почтового агента
- неожиданное уведомление антивирусной программы об обнаружении вируса
- неожиданное отключение электроэнергии

200. Сигнатурный метод антивирусной проверки заключается в …

- √ анализе поведения файла в разных условиях
- все ответы не верны
- анализе кода на предмет наличия подозрительных команд
- отправке файлов на экспертизу в компанию-производителя антивирусного средства
- сравнении файла с известными образцами вирусов

201. какие мероприятия не являются административными при обеспечении мер безопасности:

- пропускной режим
- порядок хранения документов
- √ выявление уязвимостей в системе защиты
- контроль смены паролей
- контроль журналов работы

202. Чему равен коэффициент сжатия, если начальный объем составлял 250 кбайт, после сжатия 50 кбайт

- √ 20%
- 10%
- 15 %
- 25%
- 50%

203. какого типа файлы лучше всего сжимаются:

- исполняемые

- скрытые
- текстовые
- все ответы не верны
- √ графические

204. Файловые вирусы:

- запускаются при запуске компьютера
- все ответы не верны
- √ изменяют весь код заражаемого файла
- поражают загрузочные сектора дисков
- поражают программы в начале их работы

205. Загрузочные вирусы:

- изменяют весь код заражаемого файла
- √ поражают загрузочные сектора дисков
- все ответы не верны
- запускаются при открытие файла
- запускаются при запуске компьютера

206. Отличительными особенностями компьютерного вируса являются:

- значительный объем программного кода
- все ответы верны
- необходимость запуска со стороны пользователя
- помехи корректной работе компьютера
- √ маленький объем и способность к самостоятельному запуску и созданию

207. компьютерные вирусы:

- √ создаются людьми специально для нанесения ущерба ПК
- все ответы верны
- все ответы не верны
- являются следствием ошибок в операционной системе
- зарождаются при работе неверно написанных программных продуктов

208. какое из названных действий можно произвести со сжатым файлом:

- все ответы верны
- все ответы не верны
- просмотреть
- √ распаковать
- запустить на выполнение

209. Искусственные угрозы безопасности информации вызваны:

- √ корыстными устремлениями злоумышленников;
- ошибками при действиях персонала.
- деятельностью человека;
- ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
- воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

210. Естественные угрозы безопасности информации вызваны:

- корыстными устремлениями злоумышленников;
- деятельностью человека;
- ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
- √ воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
- ошибками при действиях персонала.

211. Пользователь (потребитель) информации это:

√ субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;
- участник правоотношений в информационных процессах.
- физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
- субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
- субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

212. Атака, которая позволяет воздействовать на перехваченную информацию (проводить селекцию потока информации):

- удаленный контроль над станцией в сети.
- ложный объект распределенной вычислительной сети;
- подмена доверенного объекта или субъекта распределенной вычислительной сети;
√ анализ сетевого трафика;
- отказ в обслуживании;

213. К внутренним нарушителям информационной безопасности относится:

- клиенты.
√ посетители;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
- технический персонал, обслуживающий здание;
- любые лица, находящиеся внутри контролируемой территории;

214. К внутренним нарушителям информационной безопасности относится:

- клиенты.
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
√ сотрудники отделов разработки и сопровождения ПО;
- посетители;
- любые лица, находящиеся внутри контролируемой территории;

215. К основным непреднамеренным искусственным угрозам АСОИ относится:

√ физическое разрушение системы путем взрыва, поджога и т.п.;
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.
- нелегальное внедрение и использование неучтенных программ игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения служебных обязанностей;
- изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

216. К основным непреднамеренным искусственным угрозам АСОИ относится:

- физическое разрушение системы путем взрыва, поджога и т.п.;
√ перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.
- неумышленная порча носителей информации;
- изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

217. К основным непреднамеренным искусственным угрозам АСОИ относится:

- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.
- физическое разрушение системы путем взрыва, поджога и т.п.;
- неправомерное отключение оборудования или изменение режимов работы устройств и программ;

√ изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

218. k основным непреднамеренным искусственным угрозам АСОИ относится:

- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- √ неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.
- физическое разрушение системы путем взрыва, поджога и т.п.;
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
- изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

219. Выберите вариант, в котором единицы измерения информации расположены в порядке возрастания.

- все ответы неверны
- гигабайт, мегабайт, терабайт
- терабайт, мегабайт, гигабайт
- √ мегабайт, гигабайт, терабайт
- мегабайт, терабайт, гигабайт

220. количество информации содержащееся в одном разряде двоичного числа равно…

- все ответы неверны
- 1 байт
- 2 бита
- 2 байта
- √ 1 бит

221. В вычислительной технике в качестве основной используется _____ система счисления

- десятичная
- восьмеричная
- все ответы неверны
- шестнадцатеричная
- √ двоичная

222. Наибольшее натуральное число, кодируемое 7 битами, равно…

- все ответы неверны
- 255
- 127
- 256
- √ 128

223. В ЭВМ для записи целых положительных чисел используется ...

- все ответы неверны
- обратный код
- √ мантисса и порядок
- прямой код
- дополнительный код

224. Свойство алгоритма _____ означает, что при корректно заданных исходных данных алгоритм выдает результат за фиксированное число шагов

- детерминированность
- √ конечность
- массовость
- все ответы неверны
- понятность

225. Свойство алгоритма _____ означает, что применение алгоритма k одним и тем же данным должно давать одинаковый результат

- все ответы неверны
- √ массовость
- конечность
- результативность
- детерминированность (определенность)

226. k внутренним нарушителям информационной безопасности относится:

- посетители;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
- клиенты;
- любые лица, находящиеся внутри контролируемой территории;
- √ персонал, обслуживающий технические средства.

227. k внутренним нарушителям информационной безопасности относится:

- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
- посетители;
- √ пользователи системы;
- клиенты;
- любые лица, находящиеся внутри контролируемой территории;

228. k основным преднамеренным искусственным угрозам АСОИ относится:

- игнорирование организационных ограничений (установленных правил) при работе в системе;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).
- пересылка данных по ошибочному адресу абонента;
- √ незаконное подключение к линиям связи с целью подмены законного пользователя путем его отключения после входа в систему;
- неправомерное отключение оборудования или изменение режимов работы устройств и программ;

229. k основным преднамеренным искусственным угрозам АСОИ относится:

- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).
- пересылка данных по ошибочному адресу абонента;
- неправомерное отключение оборудования или изменение режимов работы устройств и программ;
- √ незаконное подключение к линиям связи с целью работы "между строк";
- игнорирование организационных ограничений (установленных правил) при работе в системе;

230. Энтропия в информатике – это свойство …

- все ответы неверны
- данных
- √ знаний
- условий поиска
- информации

231. хранение информации это -

- предотврашение доступа к информации лицам, не имеющим на это права
- распространение новой информации полученной в процессе научного познания
- процесс создание распределенных компьютерых баз и банков данных;
- способ распростаненния информации во времени
- √ предотвращение непредумышленного или несанкционированного использования изменения информации

232. kakово максимальное количество символов, в которых может измеряться ширина столбца в Excel:

- от 0 до 76
- от 1 до 898
- от 0 до 8
- от 0 до 409
- √ от 0 до 255

233. kakой вид расширения имеют файлы, создаваемые в Excel:

- com
- exe
- √ .xls
- .txt
- pas

234. kak называются koординаты ячейки в таблицах Excel:

- цифра
- буква
- √ адрес
- [yeni cavab]
- номер

235. kakой элемент таблицы Excel является основным:

- строка
- √ ячейка
- адрес
- информация
- столбец

236. kak называется информация, которая является результатом различных операций в таблицах Excel:

- исходная
- табличная
- рабочая
- √ производная
- первичная

237. С помощью, kakой команды в редакторе Word осуществляется набор текста в несколько колонок:

- Файл – Параметры страниц
- Таблица – Скрыть сетку
- Сервис – Параметры
- √ Формат – Колонки
- Вид – Схема документа

238. В kakом пункте горизонтального меню редактора Word находится команда Предварительный просмотр :

- Правка
- Окно
- Вид
- Сервис
- √ Файл

239. В kakом пункте горизонтального меню редактора Word находится команда Разрыв, которая позволяет установить принудительный переход на другую страницу:

- Файл

- Вид
- Сервис
- Правка

√ Вставка

240. Используя, kakой пункт горизонтального меню редактора Word, можно вставить сноску:

- Формат

√ Вид

- Файл
- Вставка
- Правка

241. В kaком пункте горизонтального меню редактора Word устанавливаются номера страниц:

- Файл
- Правка
- Формат

√ Вставка

- Вид

242. . В kaком пункте горизонтального меню редактора Word устанавливаются параметры страницы:

- Правка

√ Файл

- Сервис
- Справка
- Вид

243. При вводе больших текстов в редакторе Word для занесения элемента в список авто коррекции (автозамены), выбирают команду:

- Файл – Отправить

√ Сервис – Параметры автозамены

- Окно – Новое
- Вставка – Автотекст
- Правка – Найти

244. компьютерный вирус - это

- средство для проверке дисков
- программа
- файл который при запуске <<заражаем>> другие
- программы для отслеживания вирусов

√ специальная программа способная размножаться

245. Excel. Ячейки, которые находятся слева, справа, вверху и внизу от текущей, называются:

√ смежными

- специальными
- соседними
- встроенными
- несмежными

246. Excel. Данные в ячейке, которая должна содержать результат вычислений, начинаются с символа:

√ & =

- +
- *
- /

- \

247. Word. Чтобы вывести на экран изображение koординатной линейки, надо воспользоваться пунктом меню:

- правка
- таблица
- формат
- сервис
- √ вид

248. kakие из перечисленных элементов не присутствуют в okне приложения Word:

- горизонтальное меню
- строка заголовка
- линейки
- строка состояния
- √ кнопки диалога

249. В kakом пункте меню Word находится опция установki междустрочного интервала:

- √ формат
- сервис
- вставка
- вид
- правка

250. kakово максимальное kоличество пунktов, в kоторых измеряется высота строki в Excel:

- от 0 до 255
- √ от 0 до 409
- от 1 до 765
- от 0 до 4
- от 0 до 567
- [yeni cavab]

251. Word. Чтобы выделить предложение, надо:

- подвести курсор на предложение и, удерживая в нажатом положении клавишу ALT, щелкните правой кнопкой мыши
- √ подвести курсор на предложение и, удерживая в нажатом положении клавишу CTRL, щелкните левой кнопкой мыши
- подвести курсор на предложение и, удерживая в нажатом положении клавишу ALT, щелкните левой кнопкой мыши
- подвести курсор на предложение и, удерживая в нажатом положении клавишу SHIFT, щелкните левой кнопкой мыши
- подвести курсор на предложение и, удерживая в нажатом положении клавишу CTRL, щелкните правой кнопкой мыши

252. Word. Чтобы выделить слово, надо:

- удерживая клавишу CTRL, один раз щелкнуть по нему
- один раз щелкнуть по нему
- удерживая клавишу ALT, один раз щелкнуть по нему
- √ дважды щелкнуть по нему
- удерживая клавишу SHIFT, два раза щелкнуть по нему

253. Текст в Word нельзя выровнять:

- по левому краю
- по центру
- по ширине
- √ по длине
- по правому краю

254. Что такое тип документа:

√ расширение имени файла-документа
• название документа
• картинка, которая представляет собой какой-либо файл в Windows
• месторасположение документа на жестком диске
• объем документа

255. Excel. Абсолютный адрес ячейки это:

• обозначение ячейки, составленное из номера столбца
• обозначение ячейки, составленное буквами латинского алфавита
√ обозначение ячейки, составленное с помощью знака $ и номера столбца и (или) номера строки
• обозначение ячейки, составленное из номера столбца и номера сроки
• обозначение ячейки, составленное из номера сроки

256. Excel. kakая из формул записана правильно:

• A1+A2+A3=
√ =1A+2A
• =A1+A2+3B
• =1+A2+A3
• A1+A2+A3

257. kakoe расширение имеют графические файлы растрового формата:

• .txt
√ .bmp или .pcx
• .bat
• .arj или .rar
• .doc

258. Наиболее популярная служба Интернет:

• FTP
• Gopher
• Archie
√ E-mail
• Wais

259. Электронная почта - это:

√ сетевая служба, позволяющая обмениваться текстовыми электронными сообщениями через Интернет
• письмо, в котором можно переслать анимационные объекты, рисунки, звуки
• обыкновенное письмо, посылаемое не через почтам, а с помощью некоторого электронного оборудования
• сообщение, посылаемое только с помощью локальной сети
• письмо, в котором можно переслать текстовую информацию

260. В электронной таблице выделена группа ячеек A1:C2. Cколько ячеек входит в эту группу:

• 4
√ 6
• 5
• 3
• 7

261. Укажите элемент, характерный для окна табличного процессора Excel:

• пункт горизонтального меню «Таблица»
√ строка формул
• кнопка «Пуск»

- панель задач
- ярлыки и значки объектов

262. Рабочий лист книги Excel представляет собой:

- стандартное окно, содержащее панель Таблица и границы
- чистый лист, на котором с помощью специальных инструментов создается таблица
- произвольный шаблон таблицы
- √ готовую таблицу со столбцами, поименованными заглавными латинскими буквами и пронумерованными строками
- рабочую область папки

263. kak называется dokумент табличного процессора Excel:

- √ книгой
- пакетом
- презентацией
- страницей
- листом

264. Электронный табличный процессор Excel позволяет:

- √ обрабатывать табличные данные
- применить анимации к данным
- строить рисованные объекты различного типа
- форматировать рисунки
- форматировать данные по ширине

265. Относительный адрес ячейки это:

- обозначение ячейки, написанное буквами латинского алфавита
- обозначение ячейки, составленное из номера строки
- обозначение ячейки, составленное из номера столбца
- √ обозначение ячейки, составленное из номера столбца и номера строки
- обозначение ячейки, составленное с помощью $ и номера столбца и (или) номера строки

266. Домен – это:

- документ, который наряду с обычной текстовой и графической информацией, содержит ссылки на другие документы, причем эти ссылки встроены в текстовые фрагменты или в графические объекты данного документа
- √ общая часть имени у группы компьютеров в Интернет, она определяет место нахождение компьютера и категорию организации - владельца
- специальное имя пользователя, которое он использует в чатах
- компьютер, который предоставляет по сети данные, необходимые для работы программ
- совокупность Web-страниц, принадлежащая частному лицу или организации и размещенная на каком-либо Web-сервере

267. По умолчанию числа выравниваются в электронной таблице MS EXCEL:

- по ширине
- по длине
- √ по правому краю
- по центру
- по левому краю

268. По умолчанию текст выравнивается в электронной таблице MS EXCEL:

- по длине
- по центру
- √ по левому краю
- по ширине
- по правому краю

269. Для создания маркированного или нумерованного списков нужно:

- использовать панель Рисование
- √ выполнить команду Формат – Список – выбрать нужный тип
- использовать инструмент панели Форматирование “Кисть”
- использовать инструмент панели Рисование “Список”
- выполнить команду Вставка – Номера

270. Текстовый редактор Word позволяет создать таблицу следующим способом:

- √ команда Таблица - Вставить -Таблица
- команда Вставка – Нарисовать таблицу
- с помощью инструментов панели «Рисование»
- инструмент “Добавить таблицу” панели Рисование
- использовать карандаш панели Рисование

271. какой специальный символ используется при написании адреса электронной почты?

- 5
- #
- *
- √ @
- $

272. Для создания баз данных, а также выполнения операции поиска и сортировки данных предназначены специальные программы:

- компьютерные сети
- системы управления базами данных (СУБД)
- системы автоматического проектирования (САПР)
- библиотечные модули
- √ автоматические системы управления (АСУ)

273. Access. Что является запросом:

- запрос – это объект, предназначенный для отображения данных на бумаге
- √ запрос – это объект, предназначенный для отбора, фильтрации, сортировки данных
- запрос – это объект, предназначенный для ввода данных
- запрос – это объект, предназначенный для ввода данных и отображения их на экране
- запрос – это объект, предназначенный для форматирования данных

274. Word. Виды списков:

- ненумерованный
- немаркированный
- разветвляющийся
- линейный
- √ маркированный, нумерованный, многоуровневый

275. какая программа предназначена для работы в сети Internet?

- MS Excel
- Paint
- MS Access
- √ Internet Explorer
- MS Word

276. MS EXCEL. Чтобы подтвердить ввод формулы в ячейку, надо:

- нажать клавишу CTRL
- щелкнуть мышью на другой ячейке
- √ нажать Enter
- задать команду Файл - Сохранить
- нажать клавишу ESC

277. MS EXCEL . Создать новую рабочую книгу можно:

- запуском программы MS Word
- выбором команды Файл – Открыть
- использованием кнопки Открыть на Стандартной панели инструментов
- использованием комбинации клавиш Alt + N
- √ выбором команды Файл – Создать

278. Access. Что такое база данных:

- √ база данных – это набор данных, которые организованы специальным образом
- база данных – это набор записей и файлов, которые организованы специальным образом
- база данных – это набор символов, которые организованы специальным образом
- база данных – это набор файлов, которые организованы специальным образом
- база данных – это набор записей, которые организованы специальным образом

279. Под угрозой удаленного администрирования в компьютерной сети понимается угроза

- поставки неприемлемого содержания
- √ несанкционированного управления удаленным компьютером
- внедрения агрессивного программного кода в рамках активных объектов Web-страниц
- перехвата или подмены данных на путях транспортировки
- вмешательства в личную жизнь

280. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)

- все ответы не верны
- МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения
- МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты
- √ МЭ работают только на сетевом уровне, а СОВ – еще и на физическом
- Многократный ввод данных и сличение введенных значений

281. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …

- способна противостоять только внешним информационным угрозам
- √ с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды
- все ответы не верны
- с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
- способна противостоять только информационным угрозам, как внешним так и внутренним

282. Сервисы безопасности:

- регулирование конфликтов
- √ идентификация и аутентификация
- шифрование
- инверсия паролей
- контроль целостности

283. Методы повышения достоверности входных данных

- Введение избыточности в документ первоисточник

- Отказ от использования данных
- Замена процесса ввода значения процессом выбора значения из предлагаемого множества
- Проведение комплекса регламентных работ
- √ Использование вместо ввода значения его считывание с машиночитаемого носителя

284. Суть компрометации информации

- внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать ;
- внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
- √ несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
- все ответы не верны
- дополнительные усилия для выявления изменений и восстановления истинных сведений;

285. Для безопасного использования ресурсов в сети Интернет предназначен протокол…

- все ответы не верны
- √ HTTPS;
- IRC;
- NNTP;
- FTP.

286. Формой написания IP - адреса является запись вида:
xxx.xxx.xxx.xxx ,
где xxx - это…

- Двоичный код;
- Десятичные числа от 0 до 999;
- √ Десятичные числа от 0 до 255;
- Буквы латинского алфавита.
- все ответы не верны

287. Для правильной, полной и безошибочной передачи данных необходимо придерживаться согласованных и установленных правил, которые оговорены в _____ передачи данных.

- все ответы не верны
- Порт;
- Канал;
- √ Протокол;
- Описание.

288. Любой узел сети Интернет имеет свой уникальный IP-адрес, который состоит из _____ чисел в диапазоне от 0 до 255.

- Трех;
- все ответы не верны
- Двух.
- √ Четырех;
- Пяти;

289. Основные угрозы доступности информации:

- злонамеренное изменение данных
- разрушение или повреждение помещений
- непреднамеренные ошибки пользователей
- √ хакерская атака
- отказ программного и аппаратно обеспечения

290. Сетевым протоколом является...

- все ответы не верны

√ Набор программ;
• Инструкция;
• Набор правил;
• Программа.

291. kонцепция системы защиты от информационного оружия не должна вkлючать…

• все ответы не верны.
• средства нанесения контратаки с помощью информационного оружия
• механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры
• признаки, сигнализирующие о возможном нападении
√ процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

292. Преднамеренная угроза безопасности информации

• все ответы не верны
√ кража
• наводнение
• повреждение кабеля, по которому идет передача, в связи с погодными условиями
• ошибка разработчика

293. k внутренним нарушителям информационной безопасности относится:

• любые лица, находящиеся внутри контролируемой территории;
√ посетители;
• клиенты.
• представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
• технический персонал, обслуживающий здание;

294. k внутренним нарушителям информационной безопасности относится:

• клиенты.
√ сотрудники отделов разработки и сопровождения ПО;
• посетители;
• представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
• любые лица, находящиеся внутри контролируемой территории;

295. Заражение kомпьютерными вирусами может произойти в процессе ...

• выключения компьютера
• форматирования диска
√ работы с файлами
• печати на принтере
• все ответы не верны

296. Выберите правильный ответ из предложенных вариантов. kakие программы относятся k антивирусным?

• все ответы не верны
• MS Word, MS Excel, Norton Commander.
• MS-DOS, MS Word, AVP.
√ AVP, DrWeb, Norton AntiVirus.
• MS Word, MS Excel, Paint

297. Выберите правильный ответ из предложенных вариантов. На чем основано действие антивирусной программы?

• все ответы не верны
• На ожидании начала вирусной атаки.
√ На сравнение программных кодов с известными вирусами.
• На удалении зараженных файлов.
• На всех перечисленных

298. Выберите правильный ответ из предложенных вариантов. kakие существуют вспомогательные средства защиты?

- Аппаратные средства.
- Программные средства
- √ Аппаратные средства и антивирусные программы.
- Все перечисленное
- все ответы не верны

299. Выберите правильный ответ из предложенных вариантов. kakие существуют основные средства защиты?

- √ Резервное копирование наиболее ценных данных.
- Аппаратные средства.
- все ответы не верны
- Все перечисленное
- Программные средства

300. Выберите правильный ответ из предложенных вариантов. Что takое компьютерный вирус?

- Прикладная программа.
- все ответы не верны
- База данных.
- √ Программы, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.
- Системная программа.

301. Программа для архивации файлов - это:

- все ответы не верны
- все ответы верны
- программа для создания резервных копий файлов
- √ программа для уменьшения (сжатия) исходного объема файлов
- программа для просмотра архивных файлов

302. Троянcкой программой является...

- Вредоносная программа, которая сама не размножается, а выдает себя за что-то полезное, тем самым пытаясь побудить пользователя переписать и установить на свой компьютер программу самостоятельно.
- √ Программа, вредоносное действие которой выражается в удалении и/или модификации системных файлов компьютера;
- Программа, заражающая компьютер независимо от действий пользователя;
- Программа, проникающая на компьютер пользователя через Интернет.
- все ответы не верны

303. Вирусы могут быть:
а) загрузочными,
б) мутантами,
в) невидимками,
г) дефектными,
д) логическими.

- а, в, г;
- все ответы не верны
- б, г, д;
- в, г, д;
- √ а, б, в;

304. Под утечкой информации понимается...

- Процесс раскрытия секретной информации.
- √ Несанкционированный процесс переноса информации от источника к злоумышленнику;
- Процесс уничтожения информации;
- Непреднамеренная утрата носителя информации;

- все ответы не верны

305. Программными средствами для защиты информации в компьютерной сети являются:
1) Firewall,
2) Brandmauer,
3) Sniffer,
4) Backup.

- все ответы не верны
- √ 1 и 4;
- 2 и 3;
- 3 и 4;
- 1 и 2.

306. Результатом реализации угроз информационной безопасности может быть…

- √ Внедрение дезинформации.
- Изменение конфигурации периферийных устройств;
- Уничтожение устройств ввода/вывода;
- все ответы не верны
- Уничтожение каналов связи;

307. Электронная цифровая подпись документа позволяет решить вопрос о ____ документа(у).

- все ответы не верны
- Режиме доступа к;
- Ценности;
- √ Подлинности;
- Секретности.

308. Из перечисленного:
1) пароли доступа,
2) дескрипторы,
3) шифрование,
4) хеширование,
5) установление прав доступа,
6) запрет печати,
к средствам компьютерной защиты информации относятся:

- все ответы не верны
- 1, 4, 6;
- √ 1, 3, 5;
- 2, 4, 6;
- 4, 5, 6.

309. к антивирусным программам не относятся:

- фаги
- все ответы не верны
- мониторы
- √ интерпретаторы
- ревизоры

310. Назначение антивирусных программ, называемых детекторами:

- обнаружение и уничтожение вирусов
- все ответы не верны
- уничтожение зараженных файлов
- обнаружение компьютерных вирусов
- √ контроль возможных путей распространения компьютерных вирусов

311. Файловый вирус ...

- всегда меняет начало и длину файла
- все ответы не верны
- поражает загрузочные сектора дисков
- √ всегда изменяет код заражаемого файла
- всегда меняет длину имени файла

312. Заражение компьютерным вирусом не может произойти…

- При запуске на выполнение программного файла.
- все ответы не верны
- При открытии файла, прикрепленного к почте;
- √ При включении и выключении компьютера;
- При копировании файлов;

313. Типы методов антивирусной защиты

- практические
- теоретические
- технические
- √ программные
- организационные

314. k классу условно опасных относятся программы …

- о которых нельзя однозначно сказать, что они вредоносны
- все ответы не верны
- √ характеризующиеся способностью при срабатывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне) выполнять какое-либо действие, например, удаление файлов. В остальное время они безвредны
- которые можно выполнять только при наличии установленного антивирусного программного обеспечения
- последствия выполнения которых нельзя предугадать

315. Логические бомбы относятся k классу …

- файловых вирусов
- макровирусов
- √ условно опасных программ
- троянов
- сетевых червей

316. Деятельность клавиатурных шпионов

- находясь в оперативной памяти записывают все, что пользователь вводит с клавиатуры и передают своему хозяину
- все ответы не верны
- передают хозяину марку и тип используемой пользователем клавиатуры
- находясь в оперативной памяти следят за вводимой пользователем информацией и по команде хозяина производят нужную ему замену одних символов (или групп символов) другими
- √ находясь в оперативной памяти следят за вводимой информацией. Как только пользователь вводит некое кодовое слово, клавиатурный шпион начинает выполнять вредоносные действия, заданные автором

317. Метаморфизм – это …

- создание вирусных копий путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, ничего не делающих команд
- все ответы не верны
- √ метод маскировки от антивирусов с помощью шифрования
- метод маскировки от антивирусов с помощью многоуровневого архивирования и запаковки
- создание вирусных копий путем шифрования части кода и/или вставки в код файла дополнительных, ничего не делающих команд

318. Цель создания анонимного SMTP-сервера – для …

- распределенных вычислений сложных математических задач
- все ответы не верны
- размещения на них сайтов с порнографической или другой запрещенной информацией
- √ рассылки спама
- создания ботнета

319. Главное преимущество встроенного в Microsoft Windows XP (с установленным Service Pack 2) брандмауэра по сравнению с устанавливаемыми отдельно персональными брандмауэрами

- возможность более точно задавать исключения
- все ответы не верны
- √ более ясный и интуитивно понятный интерфейс
- отсутствие необходимости отдельно покупать его и устанавливать
- наличие более полного функционала

320. Свойство вируса, позволяющее называться ему загрузочным – способность …

- √ заражать загрузочные сектора жестких дисков
- все ответы не верны
- подсвечивать кнопку Пуск на системном блоке
- вызывать перезагрузку компьютера-жертвы
- заражать загрузочные дискеты и компакт-диски

321. Использование брандмауэров относят k … методам антивирусной защиты.

- теоретическим
- все ответы не верны
- Техническим
- √ организационным
- практическим

322. k kakому типу Использование инструкций по работе за компьютером, введенные в отдельно взятом компьютерном классе, можно отнести k … методам антивирусной защиты.

- техническим
- все ответы не верны
- теоретическим
- √ практическим
- организационным

323. Задача, выполняющая модуль планирования, входящий в антивирусный комплекс

- √ настройка расписания запуска ряда важных задач (проверки на вирусы, обновления антивирусных баз и пр.)
- все ответы не верны
- настройки параметров уведомления пользователя о важных событиях в жизни антивирусного комплекса
- определения областей работы различных задач поиска вирусов
- определения параметров взаимодействия различных компонентов антивирусного комплекса

324. Обязательные свойства любого современного антивирусного комплекса

- не мешать выполнению основных функций компьютера
- не занимать канал Интернет
- надежно защищать от вирусов
- √ быть кроссплатформенным (работать под управлением любой операционной системы)
- не занимать много системных ресурсов

325. Трояны классифицируются по …

- все ответы не верны

- методу размножения
- типу вредоносной нагрузки
- методу маскировки
- √ методу распространения

326. Стадии жизненного цикла классического трояна

- внедрение копий
- активация
- подготовка копий
- поиск объектов для заражения
- √ проникновение на чужой компьютер

327. Вирус – это программа, способная…

- √ создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению
- нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети
- все ответы верны
- все ответы не верны
- нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети: прямо или посредством других программ и/или приложения

328. Типы троянов:

- дефрагментаторы дисков
- клавиатурные шпионы
- похитители паролей
- логические бомбы
- √ утилиты скрытого удаленного управления

329. Брандмауэр (firewall) – это программа, …

- реализующая простейший антивирус для скриптов и прочих использующихся в Интернет активных элементов
- все ответы не верны
- √ которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил
- которая следит за сетевыми соединениями, регистрирует и записывает в отдельный файл подробную статистику сетевой активности
- на основе которой строится система кэширования загружаемых веб-страниц

330. Скрытые проявлениям вирусного заражения:

- неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт
- наличие на рабочем столе подозрительных ярлыков
- √ наличие в оперативной памяти подозрительных процессов
- наличие на компьютере подозрительных файлов
- подозрительная сетевая активность

331. Выполнение вредоносной программой, относящейся к классическим утилитам дозвона, вызывает …

- косвенные проявления
- √ явные проявления
- материальные проявления
- скрытые проявления
- все ответы не верны

332. Преимущества эвристического метода антивирусной проверки над сигнатурным

- существенно менее требователен к ресурсам

- позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы
- √ не требует регулярного обновления антивирусных баз
- более надежный
- все ответы не верны

333. Положительные моменты в использовании для выхода в Интернет браузера, отличного от Microsoft Internet Explorer, но аналогичного по функциональности

- все ответы не верны
- √ уменьшение вероятности заражения, поскольку большинство вредоносных программ пишутся в расчете на самый популярный браузер, коим является Microsoft Internet Explorer
- возможность одновременно работать в нескольких окнах
- возможность установить отличную от www.msn.com стартовую страницу
- уменьшение вероятности заражения, поскольку использование иного браузера может косвенно свидетельствовать об отсутствии у пользователя достаточных средств для покупки Microsoft Internet Explorer

334. Преимущества сигнатурного метода антивирусной проверки над эвристическим

- более надежный
- существенно менее требователен к ресурсам
- все ответы не верны
- √ позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы
- не требует регулярного обновления антивирусных баз

335. Ограничения, которые накладывает отсутствие на домашнем компьютере постоянного выхода в Интернет

- все ответы не верны
- невозможность использовать антиспамовую программу в режиме реального времени
- трудности с регулярным автоматическим получением новых антивирусных баз
- ложные срабатывания в работе персонального брандмауэра
- √ невозможность запуска антивирусной проверки в режиме реального времени

336. Антивирусные базы можно обновить на компьютере, не подключенном к Интернет.

- да, позвонив в службу технической поддержки компании-производителя антивирусной программы. Специалисты этой службы продиктуют последние базы, которые нужно сохранить на компьютере воспользовавшись любым текстовым редактором
- да
- нет
- √ да, это можно сделать с помощью мобильных носителей скопировав антивирусные базы с другого компьютера, на котором настроен выход в Интернет и установлена эта же антивирусная программа или на нем нужно вручную скопировать базы с сайта компании-производителя антивирусной программы
- все ответы неверны

337. Активный перехват информации это перехват, который:

- неправомерно использует технологические отходы информационного процесса;
- осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.
- √ заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
- основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
- осуществляется путем использования оптической техники;

338. Сколько процентов электронных писем являются Спамом?

- √ 10;
- 90.
- 70;
- 50;
- 30;

339. Подозрительная сетевая активность может быть вызвана …

- сетевым червем
- все ответы неверны
- логической бомбой
- трояном
- √ P2P-червем

340. Перехват, который неправомерно использует технологические отходы информационного процесса называется:

- видеоперехват;
- √ просмотр мусора.
- активный перехват;
- пассивный перехват;
- аудиоперехват;

341. Перехват, который осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера называется:

- пассивный перехват;
- √ видеоперехват;
- просмотр мусора.
- аудиоперехват;
- активный перехват;

342. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

- видеоперехват;
- просмотр мусора.
- активный перехват;
- √ пассивный перехват;
- аудиоперехват;

343. Перехват, который осуществляется путем использования оптической техники называется:

- активный перехват;
- просмотр мусора.
- √ видеоперехват;
- аудиоперехват;
- пассивный перехват;

344. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

- активный перехват;
- просмотр мусора.
- видеоперехват;
- √ аудиоперехват;
- пассивный перехват;

345. Аудиоперехват перехват информации это перехват, который:

- осуществляется путем использования оптической техники;
- осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.
- основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
- √ заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
- неправомерно использует технологические отходы информационного процесса;

346. Пассивный перехват информации это перехват, который:

- неправомерно использует технологические отходы информационного процесса;

- основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
- заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
- осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.
- √ осуществляется путем использования оптической техники;

347. Необходимость модуля обновления для любого современного антивирусного средства – для …

- √ подключения антивирусных баз к антивирусной программе
- все ответы неверны
- доставки сигнатур на компьютеры всех пользователей, использующих соответствующую антивирусную программу
- взаимодействия антивирусной программы с сайтом компании-производителя
- обеспечения взаимодействия операционной системы с антивирусным комплексом

348. Основная задача, которую решает антивирусная проверка в режиме реального времени

- обеспечение невмешательства в процесс деятельности других программ
- предоставление возможности глубокой проверки заданных объектов
- все ответы неверны
- обеспечение взаимодействия между пользователем и антивирусной программой
- √ обеспечение непрерывности антивирусной проверки

349. Просмотр мусора это перехват информации, который:

- осуществляется путем использования оптической техники;
- осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.
- основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
- заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
- √ неправомерно использует технологические отходы информационного процесса;

350. Защита информации от несанкционированного доступа это деятельность по предотвращению

- воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
- получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
- √ неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
- несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
- воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

351. Защита информации от непреднамеренного воздействия это деятельность по предотвращению:

- √ получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
- несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
- неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
- воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
- воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

352. Защита информации от несанкционированного воздействия это деятельность по предотвращению:

- получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
- √ воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
- несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

- неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
- воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

353. Защита информации от утечki это деятельность по предотвращению:

- получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
- несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
- √ неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
- воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
- воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

354. Лицо, которое взламывает интрасеть в познавательных целях это:

- фракер;
- кракер.
- скамер;
- хакер;
- √ фишер;

355. Владелец информации это:

- субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;
- участник правоотношений в информационных процессах.
- физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
- субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
- √ субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

356. Собственник информации это:

- субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
- участник правоотношений в информационных процессах.
- физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
- √ субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
- субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

357. Носитель информации это:

- √ физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
- участник правоотношений в информационных процессах.
- субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
- субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
- субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;

358. Субъект доступа k информации это:

- физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
- участник правоотношений в информационных процессах.

- субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
- √ субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
- субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;

359. Доступ k информации это:

- √ совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
- деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
- процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
- преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
- получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

360. Шифрование информации это:

- деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
- совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
- √ преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
- процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
- получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

361. Информационные процессы это:

- получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
- деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
- √ процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
- преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
- совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

362. Защита информации это:

- √ преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
- совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
- деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
- получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
- процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

363. xakep?

- Так в XIX веке называли плохого игрока в гольф, дилетанта;
- Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.
- Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
- Это лицо, которое взламывает интрасеть в познавательных целях;
- √ Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;

364. kak можно выделить весь рабочий лист в Excel:

- нажав Shift нужно щелкнуть в ярлыке листа
- дважды щелкнув в ярлыке самого первого листа
- дважды щелкнув в ярлыке последнего листа
- нажав Ctrl, нужно с помощью мыши выделить рабочий лист
- √ щелкнув в ячейке стоящей на пересечении заголовка столбцов и строк

365. kak можно удалить лист рабочей книги в Excel:

√ с помощью вызова контекстного меню в ярлычке листа и выбрать команду Удалить
• нельзя удалить лист
• на ярлыке листа нажать Backspase
• щелкнуть в ярлыке листа и нажать Delete
• дважды щелкнуть в ярлычке листа и нажать Delete

366. Excel. Чтобы отобразить/убрать строку формул и строку состояния на экране нужно:

• выполнить последовательность Сервис – Параметры – Вид и включить соответствующие флажки
• выполнить последовательность Правка – Параметры – Вид и включить соответствующие флажки
• выполнить последовательность Сервис – Вид и включить соответствующие флажки
√ выполнить последовательность Вид – Строка формул и Вид – Строка состояния и включить соответствующие флажки
• выполнить последовательность Сервис – Настройка – Вид и включить соответствующие флажки

367. Excel. какие параметры устанавливаются в мастере диаграмм в первую очередь:

√ тип диаграммы
• дополнительные элементы диаграммы
• размещение диаграммы
• размещение легенды
• диапазон данных

368. Если в меню текстового процессора Word некоторые команды сопровождаются многоточием, то это означает что:

√ они при своем выполнении вызывают подменю
• они используются наименее часто
• они используются наиболее часто
• они требуют для своего выполнения дополнительной информации
• они в данной ситуации - невыполнимы

369. какая команда в редакторе Word позволяет подобрать синонимы к словам:

√ Сервис – Язык - Тезаурус
• Формат - Шрифт
• Файл - Параметры страницы
• Вставка-Символ
• Правка - Копировать

370. Перед выводом документа Word на печать документ можно просмотреть с помощью команды:

√ Файл → Предварительный просмотр
• Вид→ Просмотр документа
• Файл → Печать→ Предварительный просмотр
• Вид → Предварительный просмотр
• Правка→ Просмотр документа

371. Для переименования рабочего листа Excel нужно:

√ дважды щелкнуть на ярлычке листа и ввести новое имя
• в меню Файл выбрать пункт Переименовать и ввести новое имя
• в меню Вид выбрать пункт Переименовать и ввести новое имя
• в меню Сервис выбрать пункт Лист и ввести новое имя
• в меню Правка выбрать пункт Переименовать и ввести новое имя

372. Excel. Чтобы выделить весь столбец, надо:

• щелкнуть по номеру строки
• щелкнуть правой кнопкой мыши
• удерживая кнопку мыши, протянуть выделение вниз
√ щелкнуть на ярлычке-заголовке

- задать команду Правка-Выделить

373. Объединить ячейки таблицы, вставленной в Word можно, если:

- выделить смежные ячейки и дважды щелкнуть правой кнопкой мыши
- объединение ячеек возможно только в Excel
- удалить одну из смежных ячеек с помощью клавиши Delete
- √ выделить смежные ячейки и воспользоваться командой Таблица - Объединить ячейки
- выделить смежные ячейки и воспользоваться командой Формат – Ячейки - Объединение

374. kakая из операций не входит в форматирование текста:

- устанавливать межсимвольные интервалы
- устанавливать шрифт
- определять эффекты в шрифтах
- √ создание таблицы
- устанавливать межстрочные интервалы

375. Документы Word сохраняются в виде файлов с расширением:

- .dbf
- .txt
- .xls
- .dot
- √ .doc

376. Access. Что является формой:

- форма – это объект, предназначенный для отображения данных на бумаге
- форма – это объект, предназначенный для отображения данных на экране
- форма – это объект, предназначенный для ввода данных
- √ форма – это объект, предназначенный для ввода данных и отображения их на экране
- форма – это объект, предназначенный для редактирования данных

377. Домен .ru является _____ доменом.

- все ответы не верны
- Основным;
- Первичным.
- Надежным;
- √ Зональным;

378. Укажите правильно записанный IP-адрес в компьютерной сети

- √ 10.172.122.26;
- 192.154.144.270;
- www.50.50.10;
- www.alfa193.com.
- 193.264.255.10;

379. Системой, автоматически устанавливающей связь между IP-адресами в сети Интернет и текстовыми именами, является ...

- все ответы не верны
- Доменная система имен (DNS);
- √ Система URL-адресации;
- Интернет-протокол;
- Протокол передачи гипертекста.

380. Адрес веб-страницы для просмотра в браузере начинается с...

√ http;
- ftp;
- www;
- smpt
- все ответы не верны

381. Протокол SMTP предназначен для…

- все ответы не верны
- Общения в чате
√ Отправки электронной почты;
- Просмотра веб-страниц;
- Приема электронной почты.

382. Поток сообщений в сети передачи данных определяется:

- Скоростью передачи данных
√ Трафиком;
- Треком;
- Объемом памяти канала передачи сообщений;
- все ответы не верны

383. Протокол POP3 работает на _____ уровне.

- Физическом;
- Сетевом;
√ Прикладном.
- все ответы не верны
- Транспортном;

384. Протокол FTP предназначен для...

- просмотра Web-страниц
√ передачи файлов
- общения в чатах
- загрузки сообщений из новостных групп
- все ответы не верны

385. Программы, которые позволяют обнаруживать файлы, зараженные одним из нескольких компьютерных вирусов, называют:

- программы-вакцины
- программы-архиваторы
- программы-вирусы
- завирусованные файлы
√ программы-детекторы

386. Виды адресации в электронной таблице Excel:

- относительная, смешанная, простая
- абсолютная, простая, смешанная
- абсолютная, смешанная, простая
√ абсолютная, относительная, смешанная
- относительная, абсолютная, простая

387. Что такое активная ячейка в Excel:

√ ячейка, выделенная табличным курсором
- последовательность ячеек
- промежуток ячеек
- смежные ячейки

- соседняя ячейка

388. kонцепция системы защиты от информационного оружия не должна вkлючать…

√ сретства нанесения контратаки с помощью информационного оружия.
- признаки, сигнализирующие о возможном нападении
- процедуры оценки уровня и особенностей атаки против национальной
- инфраструктуры в целом и отдельных пользователей
- механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры

389. Основными kомпонентами парольной системы являются
1.интервейс администратора
2.хранимая kопия пароля
3.база данных учетных записей
4.все варианты верны

√ 1,3,
- 3,4
- 2,4
- нет правильного ответа
- 2,3

390. хранение паролей может осуществляться
1.в виде сверток
2.в отkрытом виде
3.в заkрытом виде
4.в зашифрованном виде
5.все варианты ответа верны

√ 1,,2,4
- 3,4,5
- 2,4
- 2,3
- 2,3,4

391. Гарантия того, что АС ведет себя в нормальном и внештатном режиме tak, kak запланировано

√ Надеженность
- контролируемость
- устойчивость
- доступность
- точность

392. k оборонительным системам защиты относятся:
1.проволочные ограждения
2.звуkовые установkи
3.датчиkи
4.световые установkи

- 3,4
- 4
√ 1,2,,4
- 3
- 1,3,4

393. Автоматизированная система должна обеспечивать
1.надежность
2.даступность
3.целосдность
4.kонтролируемость

√ 2,3.
- 3,4
- 1,3

- нет правильного ответа
- 1,2

394. k видам системы обнаружения атак относятся :

√ все варианты верны.
- системы, обнаружения атаки на конкретные приложения
- системы, обнаружения атаки на удаленных БД
- нет правильного ответа
- системы, обнаружения атаки на ОС

395. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена

√ Конфинденциальность
- доступность
- аутентичность
- аппелеруемость
- целостность

396. Защита информации обеспечивается применением антивирусных средств

√ да
- не всегда
- всегда
- иногда
- нет

397. Информация, составляющая государственную тайну не может иметь гриф…

√ «для служебнаго пользования».
- «совершенно секретно»
- «особой важности»
- нет правильного ответа
- «секретно»

398. Наиболее эффективное средство для защиты от сетевых атак

√ использавание сетевых экранов или «firewall».
- посещение только «надёжных» Интернет-узлов
- использование только сертифицированных программ-броузеров при доступе к сети Интернет
- нет правильного ответа
- использование антивирусных программ

399. Утечка информации – это …

√ несанкцианированный процесс переноса информации от источника к злоумышленнику.
- процесс уничтожения информации
- непреднамеренная утрата носителя информации
- нет правильного ответа
- процесс раскрытия секретной информации

400. k формам защиты информации не относится…
1.аналитическая
2.правовая
3.организационно-техническая
4.страховая

√ 1,4.
- 1,3
- 3,4
- 2,4

- 1,2

401. Гарантия точного и полного выполнения kоманд в АС:

√ точнасть
- контролируемость
- устойчивость
- доступность
- надежность

402. kакие kомпоненты входят в kомплекс защиты охраняемых объектов:
1.сигнализация
2.охрана
3.датчики
4.телевизионная система

√ все варианты.
- 3,4
- 1,4
- 2,3
- 1,2

403. Из перечисленного в ОС UNIX существуют администраторы: 1) системных утилит; 2) службы kонтроля; 3) службы аутентификации; 4) тиражирования; 5) печати; 6) аудита

√ 1, 3, 5, 6.
- 1, 2, 4
- 4, 5
- 1, 2, 3

404. Из перечисленного в обязанности сотрудниkов группы информационной безопасности входят: 1) управление доступом пользователей k данным; 2) расследование причин нарушения защиты; 3) исправление ошибok в программном обеспечении; 4) устранение дефектов аппаратной части

√ 1, 2;
- 1, 3
- 3, 4
- 4
- 1, 3, 4

405. Из перечисленного базовыми услугами для обеспечения безопасности kомпьютерных систем и сетей являются: 1) аутентификация; 2) идентификация; 3) целостность; 4) kонтроль доступа; 5) kонтроль трафиka; 6) причастность

- 1, 2, 5;
- 3, 4, 5;
√ 1, 3, 4, 6.
- 1, 3, 5;
- 2, 3, 4;

406. Из перечисленного ACL-списok содержит: 1) сpok действия маркера доступа; 2) домены, kоторым разрешен доступ k объекту; 3) операции, kоторые разрешены с kаждым объектом; 4) тип доступа

√ 2, 4.
- 1, 3;
- 1, 2;
- 2,3;
- 1, 4;

407. Защита от форматирования жесткого диска со стороны пользователей обеспечивается

√ аппаратным модулем, устанавливаемым на системную шину ПК.
- специальным программным обеспечением

- аппаратным модулем, устанавливаемым на контроллер
- ПО
- системным программным обеспечением

408. Защита исполняемых файлов обеспечивается

√ обязательным контролем попытки запуска.
- специальным режимом запуска
- дополнительным хостом
- стандартным запуском
- криптографией

409. Запись определенных событий в журнал безопасности сервера называется

√ аудитом.
- мониторингом;
- учетом;
- контролем;
- трафиком;

410. Восстановление данных является дополнительной функцией услуги защиты

√ целостность.
- причастность;
- контроль доступа;
- идентификация;
- аутентификация;

411. Достоинством матричных моделей безопасности является

√ легкость представления широкого спектра правил обеспечения безопасности.
- расширенный аудит
- контроль за потоками информации
- обеспепечение безопасности
- гибкость управления

412. Для реализации технологии RAID создается

√ псевдодрайвер;
- интерпретатор
- компилятор
- аппаратные средства
- специальный процесс

413. Взаимодействие с глобальными ресурсами других организаций определяет уровень ОС

√ внешний.
- приложений;
- сетевой;
- внутренний
- системный;

414. В многоуровневой модели, если уровни безопасности субъекта и объекта доступа не сравнимы, то

√ никакие запросы на выполняются.
- выполняются запросы минимального уровня безопасности
- все запросы выполняются
- ни один запрос не выполняется
- доступ специально оговаривается

415. Средства уничтожения, иckажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа k ним это:

√ Информационное оружие
- информационное превосходство
- информационная сдача
- информационная среда
- информационная война

416. Набор аппаратных и программных средств для обеспечения сохранности, доступности и kонфиденциальности данных:

√ Компьютерная безопасность
- защищенность информации
- безопасность данных
- доступность данных
- защита информации

417. k выполняемой фунkции защиты относится:

√ все варианты верны.
- внутренняя память
- внешняя память
- внешняя защита
- внутренняя защита

418. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это…

- Защищенность информации
- Компьютерная безопасность
√ Защита информаци
- Доступность данных
- Безопасность данных

419. k вирусам изменяющим среду обитания относятся:

√ черви,
- спутники
- полиморфныее
- студенческие
- стелс

420. Выбрать недостатki имеющиеся у антивирусной программы ревизор:
1.неспособность поймать вирус в момент его появления в системе
2.небольшая ckорость поиcka вирусов
3.невозможность определить вирус в новых файлах (в электронной почте, на дискете)

√ 1,2,,3,
- 2,3
- только 1
- только 3
- 1,3

421. k тщательно kонтролируемым зонам относятся:
1.рабочее место администратора
2.архив
3.рабочее место пользователя

- только 2
- только 1
√ 1,,2,3
- 2,3
- только 3

422. k достоинствам техническких средств защиты относятся:

- √ саздание комплексных систем защиты.
- • регулярный контроль
- • нет правильного ответа
- • все варианты верны
- • степень сложности устройства

423. Преднамеренная угроза безопасности информации

- √ кража.
- • нет правильного ответа
- • ошибка разработчика
- • повреждение кабеля, по которому идет передача, в связи с погодными условиями
- • наводнение

424. kakие степени сложности устройства Вам известны
1.упрощенные
2.простые
3.сложные
4.оптические
5.встроенные

- • только 3
- • только 1
- √ 2,3,
- • 3,4
- • 1,3

425. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …

- • вмешательства в личную жизнь
- • поставки неприемлемого содержания
- √ несанкционированнаго управления удаленным компьютером.
- • внедрения агрессивного программного кода в рамках активных объектов Web-страниц
- • перехвата или подмены данных на путях транспортировки

426. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …

- • способна противостоять только информационным угрозам, как внешним так и внутренним
- • способна противостоять только внешним информационным угрозам
- √ с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды.
- • Ничего не верно
- • с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации

427. Система физическоой безопасности включает в себя следующие подсистемы:1.оценка обстановки
2.скрытность
3.строительные препятствия
4.аварийная и пожарная сигнализация

- √ 2,3,4.
- • только 2
- • только 4
- • 1,2,4
- • 1,3,4

428. k принципам информационной безопасности относятся
1.скрытость
2.масштабность
3.системность
4.законность
5.открытости алгоритмов

√ 1,2,3
- 3,4,5
- 2,3
- 2,3,4
- 4,5,6

429. k вирусам не изменяющим среду обитания относятся:
1.черви
2.студенческие
3.полиморфные
4.спутники

√ 1,4
- 3
- 2,3
- 3,4
- 2,4

430. Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:

√ коммерческаяя тайна
- неконфиденциальная информация
- конфиденциальная информация
- банковская тайна
- государственная тайна

431. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:

- Безопасность АС
- Угроза информационной безопасности
- атака на автоматизированную систему
√ палитика безопасности.
- Комплексное обеспечение информационной безопасности

432. Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:

√ Принцип разумной достаточности
- принцип непрерывности
- принцип комплексности
- принцип системности
- принцип гибкости системы

433. Недостатком модели политики безопасности на основе анализа угроз системе является

√ изначальное допущение вскрываемости системы.
- необходимость дополнительного обучения персонала
- механизм реализации
- статичность
- сложный механизм реализации

434. k типам угроз безопасности парольных систем относятся

- тотальный перебор
- словарная атака

√ все варианты ответа верны.
• разглашение параметров учетной записи
• атака на основе психологии

435. Наименее затратный криптоанализ для криптоалгоритма RSA

√ разложение числа на простые множители.
• на сложные множители
• разложение числа на сложные множители
• перебор по выборочному ключевому пространству
• перебор по всему ключевому пространству

436. Надежность СЗИ определяется

√ Самым слабым звеном
• сильным звеном
• самым сильным звеном
• усредненным показателем
• количеством отраженных атак

437. конечное множество используемых для кодирования информации знаков называется

• шифром
• символом
√ алфавитом.
• кодом
• ключом

438. Недостатком дискретных моделей политики безопасности является

• сложный механизм реализации,
• допущение вскрываемости системы,
√ статичность.
• необходимость дополнительного обучения персонала,
• изначальное допущение вскрываемости системы,

439. Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты

• ограниченной компетенцией злоумышленника
• фиксированным ресурсом
√ за определенное время.
• фиксированным компетенцией
• фиксированными затратами

440. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет

√ криптоанализ.
• стеганология
• криптология
• стеганография
• криптография

441. Охранное освещение бывает:
a.дежуррное
b.световое
c.тревожжное

√ a,c.
• b,c
• b

- a
- a,b

442. Особенностями информационного оружия являются:
1.системность
2.открытость
3.универсальность
4.скрытность

- √ 3,4,
- только 4
- 1,4
- 2,3
- 1,2

443. k механическим системам защиты относятся:
1.проволока
2.стена
3.сигнализация
4.вы

- √ 1,2,4
- 4
- 2,3
- 3,4
- 2,3,4

444. Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно тот человек, который заявлен как ее автор и ни кто другой:

- √ Аппелируемость.
- Доступность
- Целостность
- Конфиденциальность
- Аутентичность

445. Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте:

- √ Банковская тйна
- Информационная безопасность
- Государственная тайна
- Коммерческая тайна
- Конфиденциальная информация

446. Действия предпринимаемые для достижения информационного превосходства в поддержке национальной информационной стратегии посредством воздействия на информацию и информационные системы противника:

- √ Информационная вйна
- Информационное превосходство
- Информационная безопасность
- Информационное вычисление
- Информационное оружие

447. Согласование разнородных средств при построении целостной системы защиты, перекрывающий все существенные каналы реализации угроз и не содержащий слабых мест на стыках отдельных компонентов:

- √ Принцп комплексности
- Принцип разумной достаточности
- Принцип гибкости системы
- Принцип системности
- Принцип непрерывной защиты

448. Гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор:

√ Аутентчность
• Доступность
• Целостность
• Конфиденциальность
• Аппелируемость

449. Обобщение интересов личности в этой сфере, упрочнение демокpатии, создание правового государства это:

√ Интресы общества
• Интересы государства в информационной сфере
• Интересы государства
• Интересы общества в информационной сфере
• Интересы личности в информационной сфере

450. Область науки и техники, охватывающая совокупность криптографических, программно-аппаратных, технических, правовых, организационных методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий

√ Комплексное обспечение информационной безопасности
• Угроза безопасности
• Атака на автоматизированную систему
• Политика безопасности
• Безопасность АС

451. Системный подход к защите компьютерных систем предполагающий необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:

√ Принцип систмности
• Принцип непрерывной защиты
• Принцип разумной достаточности
• Принцип гибкости системы
• Принцип комплексности

452. к какому уровню доступа информации относится следующая информация: Библиографические и опознавательные данные, личные характеристики , сведения о семейном положении, сведения об имущественном или финансовом состоянии…

√ Информация с огрниченным доступом
• Объект интеллектуальной собственности
• Иная общедоступная информация
• Информация без ограничения права доступа
• Информация, распространение которой наносит вред интересам общества

453. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов и требований:

√ Защищаемая информация
• Защищенность потребителей информации
• Защита информации
• Информационная защита
• Защищенность информации

454. Действие субъектов по обеспечению пользователей информационными продуктами:

√ Инфрмационные услуги
• Информационная система
• Информационные ресурсы
• Информационные продукты
• Информационная сфера

455. Защищаемые государством сведения в области военной, внешнеполитическоk и внешнеэкономическоk деятельности, распространение kоторых может нанести ущерб безопасности РФ.

√ Государствнная тайна
• Банковская тайна
• Конфиденциальная информация
• Конфиденциальность
• Коммерческая тайна

456. Возможность сбора, обработki и распространения непрерывного потоka информации при воспрещении использования информации противникoм это:

√ Информационное превсходство
• Информационная война
• Информационное вычисление
• Информационная безопасность
• Информационное оружие

457. Защищенность от негативных информационно-психологическux и информационно- технических воздействий:

√ Защищенность потребителей информации
• Компьютерная безопасность
• Защита информации
• Безопасность
• Защищенность информации

458. Защищенность страны от нападения извне, шпионажа, пokушения на государственный и общественный строй:

• Национальная безпасность
• Безопасность
√ Информационная безопасность
• Государственная безопасность
• Национальная безпасность

459. k kakому уровню доступа информации относится следующая информация: Ложная peklama, peklama co ckрытыми вставkами…

√ Информция , распространение которой наносит вред интересам общества
• Информация с ограниченным доступом
• Объект интеллектуальной собственности
• Иная общедоступная информация
• Информация без ограничения права доступа

460. Гарантия того, что при умышленном внесении ошибok в пределах заранее оговоренных норм АС будет вести себя tak, kak оговорено заранее:

√ Устйчивость
• точность
• Надежность
• Доступность
• Контролируемость

461. Из kakих четырех доменов состоит CobiT?

√ Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка.
• Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
• Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
• Приобретение и Внедрение, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
• Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

462. Что takое CobiT и kak он относится k разработke систем информационной безопасности и программ безопасности?

- Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
- Список стандартов, процедур и политик для разработки программы безопасности
- Текущая версия ISO 27000
- √ Открытый стандарт. определяющий цели контроля
- Текущая версия ISO 17799

463. Что представляет собой стандарт ISO/IEC 27799?

- √ Стандарт по защите персональных данных о здоровье.
- Определения для новой серии ISO 27000
- Новая версия NIST 800-60
- Новая версия ISO 17799
- Новая версия BS 17799

464. kakой из следующих zakонодательных терминов относится k компании или человеky, выполняющему необходимые действия, и используется для определения обязательств?

- √ Должная забота (Due care.)
- Стандарты
- Снижение обязательств
- Повышение обязательств
- Должный процесс (Due process)

465. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется tak много времени для проведения анализа?

- √ Много информации нужно собрать и ввести в программу.
- Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
- Множество людей должно одобрить данные
- Сотрудники должны одобрить создание группы
- Руководство должно одобрить создание группы

466. Что является наилучшим описанием kоличественного анализа рисков?

- √ Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков.
- Анализ, основанный на информации, выявленной при оценке рисков
- Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
- Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
- Метод, основанный на суждениях и интуиции

467. Защищенность АС от случайного или преднамеренного вмешательства в нормальный процесс ее фунkционирования, а takже от попыток хищения, изменения или разрушения ее kомпонентов:

- √ Безопсность АС
- Угроза информационной безопасности
- Атака на автоматизированную систему
- Политика безопасности
- Комплексное обеспечение информационной безопасности

468. Почему при проведении анализа информационных рисков следует привлеkать k этому специалистов из различных подразделений kомпании?

- √ Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа.
- Чтобы убедиться, что проводится справедливая оценка
- Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку
- Руководство должно одобрить создание группы
- Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

469. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

√ COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень.
- COSO учитывает корпоративную культуру и разработку политик
- COSO – это система отказоустойчивости
- COSO – это система управления рисками
- COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам

470. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

√ аудиоперехват.
- просмотр мусора;
- активный перехват;
- пассивный перехват;
- видеоперехват;

471. Перехват, который осуществляется путем использования оптической техники называется:

√ видеоперехват.
- пассивный перехват;
- аудиоперехват;
- просмотр мусора;
- активный перехват;

472. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

√ пассивный перехват.
- аудиоперехват;
- видеоперехват;
- просмотр мусора;
- активный перехват;

473. Антивирус не только находит зараженные вирусами файлы, но и лечит их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

√ доктор.
- ревизор;
- сторож;
- детектор;
- сканер;

474. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

√ сторож.
- сканер;
- доктор;
- детектор;
- ревизор;

475. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

- сканер;
√ ревизор.
- сторож;
- детектор;
- доктор;

476. Основные угрозы доступности информации:
1.непреднамеренные ошибki пользователей
2.злонамеренное изменение данных
3.xakepckая ataka
4.otkaз программного и аппаратно обеспечения
5.разрушение или повреждение помещений
6.перехват данных

√ 1,4,,5
- 2,3,4
- 3,4,5
- 3,4,5
- 3,5,6
- 2,3,6

477. k внутренним нарушителям информационной безопасности относится:
клиенты;

√ технический персонал, обслуживающий здание.
- любые лица, находящиеся внутри контролируемой территории;
- посетители;
- пользователи системы;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации

478. Что является наилучшим описанием kоличественного анализа pickов?
ему

√ Количественные измерения должны применяться к качественным элементам.
- Он присваивает уровни критичности. Их сложно перевести в денежный вид
- Он достижим и используется
- Множество людей должно одобрить данные
- Это связано с точностью количественных элементов

479. kak рассчитать остаточный pick?

√ (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля.
- (Угрозы х Ценность актива х Уязвимости) х Риски
- Угрозы х Риски х Ценность актива
- (Угрозы х Ценность актива) х Риски
- SLE х Частоту = ALE

480. Фунkциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

√ Уровень доверия, обеспечиваемый механизмом безопасности.
- Внедрение управления механизмами безопасности
- Выявление рисков
- Соотношение затрат / выгод
- Классификацию данных после внедрения механизмов безопасности

481. kakoe утверждение является правильным, если взглянуть на разницу в целях безопасности для kоммерческой и военной организации?

√ Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности.
- Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности
- Руководство должно одобрить создание группы
- Только военные имеют настоящую безопасность
- Военным требуется больший уровень безопасности, т.к. их риски существенно выше

482. Эффективная программа безопасности требует сбалансированного применения:

√ Технических и нетехнческих методов
- Физической безопасности и технических средств защиты

- Процедур безопасности и шифрования
- Соотношения затрат / выгод
- Контрмер и защитных механизмов

483. Что является определением воздействия (exposure) на безопасность?

√ Нечто, приводящее к ущербу от угрозы.
- Любой недостаток или отсутствие информационной безопасности
- Потенциальные потери от угрозы
- Контрмер и защитные механизмы
- Любая потенциальная опасность для информации или систем

484. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

√ Выполнение анализа рисков.
- Делегирование полномочий
- Поддержка
- Выявление рисков
- Определение цели и границ

485. Что из перечисленного не является целью проведения анализа рисков?

√ Делегирование полномочий.
- Выявление рисков
- Определение баланса между воздействием риска и стоимостью необходимых контрмер
- Определение цели и границ
- Количественная оценка воздействия потенциальных угроз

486. какая из приведенных техник является самой важной при выборе конкретных защитных мер?

√ Анализ затрат./ выгоды
- Результаты ALE
- Выявление уязвимостей и угроз, являющихся причиной риска
- Анализ действий
- Анализ рисков

487. когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

√ Когда стоимость контрмер превышает ценность актива и потенциальные потери.
- Когда риски не могут быть приняты во внимание по политическим соображениям
- Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
- Когда необходимые защитные меры слишком просты
- Когда необходимые защитные меры слишком сложны

488. Что лучше всего описывает цель расчета ALE?

- Выявление уязвимостей и угроз, являющихся причиной риска
- Количественно оценить затраты / выгоды
- Оценить возможные потери для каждой контрмеры
- Количественно оценить уровень безопасности среды

√ Оценить потенциальные потери от угрозы в год.

489. какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

√ Поддержка высшго руководства
- Актуальные и адекватные политики и процедуры безопасности
- Проведение тренингов по безопасности для всех сотрудников
- Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
- Эффективные защитные меры и методы их внедрения

490. Что такое политики безопасности?

- √ Широкие, высокоуровневые заявления руководства.
- • Общие руководящие требования по достижению определенного уровня безопасности
- • Детализированные документы по обработке инцидентов безопасности
- • Правила использования программного и аппаратного обеспечения в компании
- • Пошаговые инструкции по выполнению задач безопасности

491. Что такое процедура?

- √ Пошаговая инструкция по выполнению задачи.
- • Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
- • Обязательные действия
- • Эффективные защитные меры и методы их внедрения
- • Правила использования программного и аппаратного обеспечения в компании

492. Что самое главное должно продумать руководство при классификации данных?

- √ Необходимый уровень доступности, целостности и конфиденциальности.
- • Оценить уровень риска и отменить контрмеры
- • Управление доступом, которое должно защищать данные
- • Проведение тренингов по безопасности для всех сотрудников
- • Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

493. кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

- √ Руководтво
- • Пользователи
- • Владельцы данных
- • Сотрудники
- • Администраторы

494. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

- √ Улучшить контроль за безопасностью этой информации.
- • Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- • Снизить уровень классификации этой информации
- • Всегда требовать специального разрешения
- • Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

495. Активный перехват информации это перехват, который:

- √ осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.
- • основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники
- • заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
- • коммуникаций;
- • неправомерно использует технологические отходы информационного процесса;

496. Тактическое планирование – это:

- √ Среднесрочное планирвание
- • Ежедневное планирование
- • Планирование на 6 месяцев
- • Планирование на год
- • Долгосрочное планирование

497. какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

√ Сотрудники.
- Атакующие
- Контрагенты (лица, работающие по договору)
- Пользователи
- Хакеры

498. kто является основным ответственным за определение уровня kлассификации информации?

√ Владелец.
- Руководитель среднего звена
- Проектировщик
- Пользователь
- Высшее руководство

499. k kакому уровню доступа информации относится следующая информация: Информация в области работ по хранению, перевозke, уничтожению химическkого оружия – сведения о состоянии здоровья граждан и объектов окружающей среды в районах размещения объектов по уничтожению химическkого оружия…

√ Информация с ограниченным дступом
- Информация, распространение которой наносит вред интересам общества
- Объект интеллектуальной собственности
- Иная общедоступная информация
- Информация без ограничения права доступа

500. Dокументированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей:

√ Информационные прдукты
- Информационные услуги
- Информационные ресурсы
- Информационная система
- Информационная сфера